BayRS Version 12.10 Document Change Notice

Router Software Version 12.10
Site Manager Software Version 6.10
BCC Version 3.20

Part No. 300020-A Rev. 00
February 1998

Bay Networks

Bay Networks

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1998 Bay Networks, Inc.

All rights reserved. Printed in the USA. February 1998.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Trademarks

AN, BN, BNX, and Bay Networks are registered trademarks and ANH, ARN, ASN, BayStack, BCC, Bay Networks Press, and the Bay Networks logo are trademarks of Bay Networks, Inc.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Bay Networks, Inc. Software License Agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as “Software” in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH BAY NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these

terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License Grant. Bay Networks, Inc. (“Bay Networks”) grants the end user of the Software (“Licensee”) a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Bay Networks Agent software or other Bay Networks software products. Bay Networks Agent software or other Bay Networks software products are licensed for use under the terms of the applicable Bay Networks, Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Bay Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Bay Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Bay Networks’ and its licensors’ confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Bay Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee’s facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Bay Networks warrants each item of Software, as delivered by Bay Networks and properly installed and operated on Bay Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Bay Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Bay Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Bay Networks will replace defective media at no charge if it is returned to Bay Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee’s intended results and for the installation, use, and results obtained from the Software. Bay Networks does not warrant a) that the functions contained in the software will meet the Licensee’s requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Bay Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Bay Networks or in accordance with its instructions; (ii) used in conjunction with another vendor’s product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL BAY NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF BAY NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT

SHALL THE LIABILITY OF BAY NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO BAY NETWORKS FOR THE SOFTWARE LICENSE.

5. Government Licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of Software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Bay Networks of any such intended examination of the Software and may procure support and assistance from Bay Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Bay Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Bay Networks copyright; those restrictions relating to use and disclosure of Bay Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Bay Networks the Software, user manuals, and all copies. Bay Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and Re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Bay Networks, Inc., 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN BAY NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST BAY NETWORKS UNLESS BAY NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

About This Guide

Conventions xv
Bay Networks Technical Publications xvi
Bay Networks Customer Service xvii
How to Get Help xvii
Bay Networks Educational Services xviii

Document Change Notice

Cable Guide 3
Quad MCT1 15-Pin to 15-Pin Crossover Cable (Order No. AA0018021) 4
Quad MCT1 15-Pin to 15-Pin Straight-Through Cable (Order No. AA0018022) 5
44-Pin to F V.35 Synchronous Pass-Through Cable (Order No. 7944) 6
50-Pin to F V.35 Synchronous Pass-Through Cable (Order No. 7946) 7
Configuring ATM Services 9
Change in ATM MAC Address Override Parameter Usage 9
Defining Redundant LES/BUS Addresses 9
Enabling a LES/BUS Entry 10
Entering a LES/BUS ATM Address 10
Adding a LES/BUS Address 11
Inserting a LES/BUS Address out of Sequence 13
Modifying a LES/BUS Entry 14
Deleting a LES/BUS Entry 15
LES/BUS Parameter Descriptions 16
Configuring BayStack Remote Access 17
Configuring DECnet Services 18
Adjacent Host Address Parameter 18
Configuring Dial Services 19
Before You Begin 19

Bandwidth-on-Demand Overview 19
New Data Compression Protocol for All Three Dial Services 19
Bandwidth-on-Demand Congestion Monitor Parameters 19
Configuring DLSw Services 20
DLSw/APPN Boundary Function 20
DLSw/APPN Network Configurations 21
DLSw/APPN Components 22
Configuring the DLSw/APPN Boundary Function 25
Disabling and Reenabling the Boundary Function 29
IP Multicast Support for DLSw Version 2.0 30
Configuring DLSw in RFC 2166 Multicast Mode 30
Configuring IP Multicast Protocols on the Router 31
Assigning an IP Multicast Group Address to a Slot 31
Sample Connection Using DLSw and IP Multicasting 34
Using Site Manager to Configure DLSw for IP Multicasting 35
Configuring Ethernet, FDDI, and Token Ring Services 36
CSMA/CD Line Parameters 37
Configuring IP Multicasting and Multimedia Services 38
Guidelines for Configuring IP Multicasting and Multimedia Services 38
Configuring MOSPF, QOSPF, and DVMRP 39
Monitoring MOSPF 40
Monitoring DVMRP 40
Configuring the Expanding Ring Search 41
Configuring Administratively Scoped Multicast 41
Configuring the Static Forwarding Entry 41
Configuring the DVMRP Prune Lifetime 41
Configuring Multicasting Policies 42
Configuring IP Multicasting and Multimedia Services with Site Manager 42
Announce Policy Parameters for Both DVMRP and MOSPF 42
DVMRP-Specific Announce Policy Parameters 47
IGMP Group Policy Parameters 48
MTM Static Forwarding Policy Parameters 52
IGMP Boundary Group Parameters 55
Configuring IP Services 57
Customizing the IP Routing Table Structure 57

Configuring IPv6 Services 58
RIPv6 Announce Policy Parameters 58
IPV6 Interface Parameters 60
Configuring PPP Services 62
Summary of PPP Services 62
Priority Queueing over PPP Multilink 62
WCP over PPP Multilink 62
RFC 1661 Compliance for PPP Dial Circuits 63
Configuring X.25 Services 64
Remote Backup IP Interface for IPEX 64
Calling Address Insertion 65
Event Messages for Routers 67
AHB Fault Events 69
AHB Warning Events 73
AHB Info Events 75
ATM_LE Warning Events 77
ATM_LE Info Events 77
CSMACD Info Event 78
DCMMW Fault Event 78
DCMMW Warning Events 80
DP Warning Events 80
DP Info Events 82
DP Trace Event 84
FRPT Fault Event 84
FRPT Warning Events 85
FRPT Info Events 86
FRPT Trace Event 89
FR_SVC Fault Event 90
FR_SVC Warning Event 90
FR_SVC Info Events 91
FR_SVC_API Warning Events 92
FR_SVC_API Info Events 94
FR_SVC_API Trace Events 95
HTTP Fault Event 96
HTTP Warning Events 96

HTTP Info Events 97
HTTP Trace Events 98
ISDB Fault Events 102
ISDB Warning Events 103
ISDB Info Events 105
L2TP Fault Event 108
L2TP Warning Events 108
L2TP Info Events 111
L2TP Trace Events 114
LB Warning Event 116
LOADER Info Events 116
OSPF Fault Events 117
OSPF Warning Events 118
OSPF Info Event 119
PPP Warning Events 119
RFWALL Warning Events 120
RFWALL Info Events 121
RFWALL Trace Event 121
RMONSTAT Info Events 122
STAC Fault Event 122
STAC Warning Events 123
STAC Info Events 124
STAC Trace Event 125
TELNET Fault Event 125
TELNET Warning Events 126
TELNET Info Events 126
TELNET Trace Events 129
VCCT Fault Event 130
X.25 PAD Fault Event 130
X.25 PAD Warning Events 131
X.25 PAD Info Event 131
X.25 PAD Trace Event 132
Mananging Your Network Using the HTTP Server 132
Viewing HTTP Statistics Using Statistics Manager 132
Troubleshooting Routers 133

Troubleshooting an FT1 Connection 133
Upgrading Routers from Version 7-11.xx to Version 12.00 135
BOOT and Diagnostic PROM Upgrades for Version 12.10 135
Using the Bay Command Console (AN/BN Routers) 136
Obtaining the Version of a Help File on a Router 136
Help Updates 136
Using Technician Interface Scripts 138
show ahb 138
show fr 144
show fwall 153
show l2tp 156
show lane les 161
show mospf 162
show ospf 164
show ppp 167
show sr 168
show stac 169
show sync 171
stac enable/disable 175
Using Technician Interface Software 175
Output Change to ping -p 175

Figures

Figure 1. ATM LES List Window 10
Figure 2. LANE Redundancy Window 11
Figure 3. Data Center APPN Network 21
Figure 4. Enterprise APPN Network 22
Figure 5. Boundary Function Virtual Circuit 23
Figure 6. End-to-End Connection Using a DLSw/APPN Router and a DLSw Router 24
Figure 7. Addressing a Message to an IP Multicast Group 32
Figure 8. Receiving a Message Addressed to a Multicast Group 33
Figure 9. Multicast DLSw 34

Tables

Table 1. 12.00 and 12.10 Documentation 1
Table 2. New and Amended Event Messages 67
Table 3. Boot and Diagnostic PROMs for BayRS Version 12.10 135

About This Guide

If you are responsible for configuring and managing Bay Networks® routers, you need to read this guide to learn about changes to router software and hardware documentation since release 12.00. Table 1 of this guide lists the manuals included in the 12.10 release, identifies new and revised manuals since release 12.00, and lists those manuals that we have not revised and which are affected by sections in this document change notice.

Conventions

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: if command syntax is **ping** *<ip_address>*, you enter **ping 192.32.10.12**
bold text	Indicates text that you need to enter, command names, and buttons in menu paths. Example: Enter **wfsm &**
	Example: Use the **dinfo** command.
	Example: ATM DXI > Interfaces > **PVCs** identifies the PVCs button in the window that appears when you select the Interfaces option from the ATM DXI menu.
brackets ([ ])	Indicate optional elements. You can choose none, one, or all of the options.
italic text	Indicates variable values in command syntax descriptions, new terms, file and directory names, and book titles.
quotation marks (“ ”)	Indicate the title of a chapter or section within a book.

`screen text`	Indicates data that appears on the screen. Example: `Set Bay Networks Trap Monitor Filters`
separator (>)	Separates menu and option names in instructions and internal pin-to-pin wire connections. Example: Protocols > AppleTalk identifies the AppleTalk option in the Protocols menu. Example: Pin 7 > 19 > 20
vertical line (|)	Indicates that you enter only one of the parts of the command. The vertical line separates choices. Do not type the vertical line when entering the command. Example: If the command syntax is **show at routes** | **nets**, you enter either **show at routes** or **show at nets**, but not both.

Bay Networks Technical Publications

You can now print technical manuals and release notes free, directly from the Internet. Go to *support.baynetworks.com/library/tpubs*. Find the Bay Networks products for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Using Adobe Acrobat Reader, you can open the manuals and release notes, search for the sections you need, and print them on most standard printers. You can download Acrobat Reader free from the Adobe Systems Web site, *www.adobe.com*.

Documentation sets and CDs are available through your local Bay Networks sales office or account representative.

Bay Networks Customer Service

You can purchase a support contract from your Bay Networks distributor or authorized reseller, or directly from Bay Networks Services. For information about, or to purchase a Bay Networks service contract, either call your local Bay Networks field sales office or one of the following numbers:

Region	Telephone number	Fax number
United States and Canada	800-2LANWAN; then enter Express Routing Code (ERC) 290, when prompted, to purchase or renew a service contract 978-916-8880 (direct)	978-916-3514
Europe	33-4-92-96-69-66	33-4-92-96-69-96
Asia/Pacific	61-2-9927-8888	61-2-9927-8899
Latin America	561-988-7661	561-988-7550

Information about customer service is also available on the World Wide Web at *support.baynetworks.com*.

How to Get Help

If you purchased a service contract for your Bay Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Bay Networks service program, call one of the following Bay Networks Technical Solutions Centers:

Technical Solutions Center	Telephone number	Fax number
Billerica, MA	800-2LANWAN	978-916-3514
Santa Clara, CA	800-2LANWAN	408-495-1188
Valbonne, France	33-4-92-96-69-68	33-4-92-96-69-98
Sydney, Australia	61-2-9927-8800	61-2-9927-8811
Tokyo, Japan	81-3-5402-0180	81-3-5402-0173

Bay Networks Educational Services

Through Bay Networks Educational Services, you can attend classes and purchase CDs, videos, and computer-based training programs about Bay Networks products. Training programs can take place at your site or at a Bay Networks location. For more information about training programs, call one of the following numbers:

Region	Telephone number
United States and Canada	800-2LANWAN; then enter Express Routing Code (ERC) 282 when prompted 978-916-3460 (direct)
Europe, Middle East, and Africa	33-4-92-96-15-83
Asia/Pacific	61-2-9927-8822
Tokyo and Japan	81-3-5402-7041

Document Change Notice

Table 1 lists the manuals included in the 12.10/6.10 release and those manuals affected by sections in this document change notice.

Table 1. 12.00 and 12.10 Documentation

Document Title	New or Revised Book for 12.10/6.10	Affected by Section in DCN
Cable Guide		✔
Configuring AppleTalk Services		
Configuring APPN Services		
Configuring and Managing Routers with Site Manager		
Configuring ATM DXI Services		
Configuring ATM Services		✔
Configuring ATM Half-Bridge Services	✔	
Configuring BaySecure FireWall-1	✔	
Configuring BayStack Remote Access		✔
Configuring Bridging Services		
Configuring BSC Transport Services		
Configuring Data Compression Services	✔	
Configuring Data Encryption Services	✔	
Configuring DECnet Services		✔
Configuring Dial Services		✔
Configuring DLSw Services		✔

(continued)

Table 1. 12.00 and 12.10 Documentation *(continued)*

Document Title	New or Revised Book for 12.10/6.10	Affected by Section in DCN
Configuring Ethernet, FDDI, and Token Ring Services		✔
Configuring Frame Relay Services	✔	
Configuring Interface and Router Redundancy		
Configuring IP Multicasting and Multimedia Services		✔
Configuring IP Services	✔	✔
Configuring IP Utilities		
Configuring IPv6 Services		✔
Configuring IPX Services		
Configuring L2TP Services	✔	
Configuring LLC Services		
Configuring LNM Services		
Configuring OSI Services		
Configuring Polled AOT Transport Services		
Configuring PPP Services		✔
Configuring RADIUS		
Configuring RMON and RMON2	✔	
Configuring SDLC Services		
Configuring SMDS		
Configuring SNMP, BootP, DHCP, and RARP Services	✔	
Configuring Traffic Filters and Protocol Prioritization		
Configuring VINES Services		
Configuring WAN Line Services	✔	
Configuring XNS Services		
Configuring X.25 Gateway Services		
Configuring X.25 Services	✔	✔

(continued)

Table 1. 12.00 and 12.10 Documentation *(continued)*

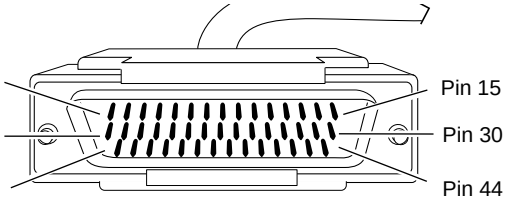
Document Title	New or Revised Book for 12.10/6.10	Affected by Section in DCN
Connecting ASN Routers to a Network		
Event Messages for Routers		✔
Managing Your Network Using the HTTP Server	✔	✔
Quick-Starting Routers	✔	
Troubleshooting Routers		✔
Upgrading Routers from Version 7-11.xx to Version 12.0 0		✔
Using the Bay Command Console (AN/BN Routers)		✔
Using Technician Interface Scripts		✔
Using Technicial Interface Software		✔
Writing Technician Interface Scripts		

Cable Guide

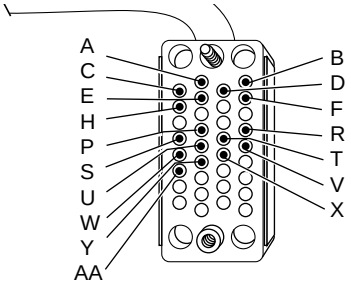
The following sections are ammendments to the *Cable Guide*:

- Quad MCT1 15-Pin to 15-Pin Crossover Cable (Order No. AA018021)
- Quad MCT1 15-Pin to 15-Pin Straight-Through Cable (Order No. AA0018022)
- 44-Pin to F V.35 Synchronous Pass-Through (Order No. 7944)
- 50-Pin to F V.35 Synchronous Pass-Through (Order No. 7946)

Quad MCT1 15-Pin to 15-Pin Crossover Cable (Order No. AA0018021)



44-position D-sub plug with screw locks
(ground shield connected to backshell)



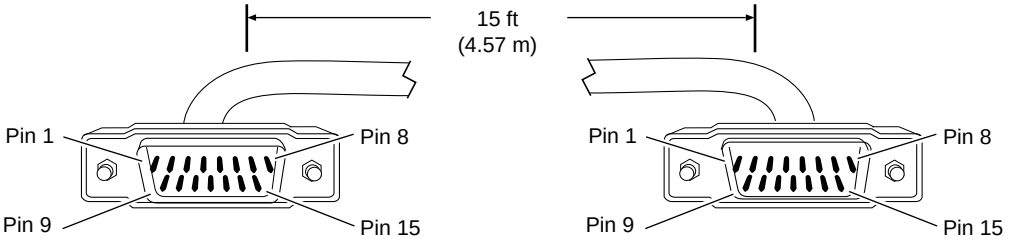
34-position V.35 receptacle with screw jack retainers
(ground shield connected to backshell)

Industry Interface Type: T1/DS1

Bay Networks Termination A		**Bay Networks Termination B**
Signal	**Pin # to Pin #**	**Signal**
Transmit Tip	1 to 3	Receive Tip
Transmit Ring	9 to 11	Receive Ring
Receive Tip	3 to 1	Transmit Tip
Receive Ring	11 to 9	Transmit Ring
Ground	2 to 4	Ground*
Ground	4 to 2	Ground*

* You must configure onboard jumpers to complete this connection. Refer to the table called "QMCT1 Link Module Settings" in *Installing T1 Link Modules in BN Platforms*.

Quad MCT1 15-Pin to 15-Pin Straight-Through Cable (Order No. AA0018022)



15-position D-sub plug with locking posts (ground shield connected to backshell)

15-position D-sub plug with locking posts (ground shield connected to backshell)

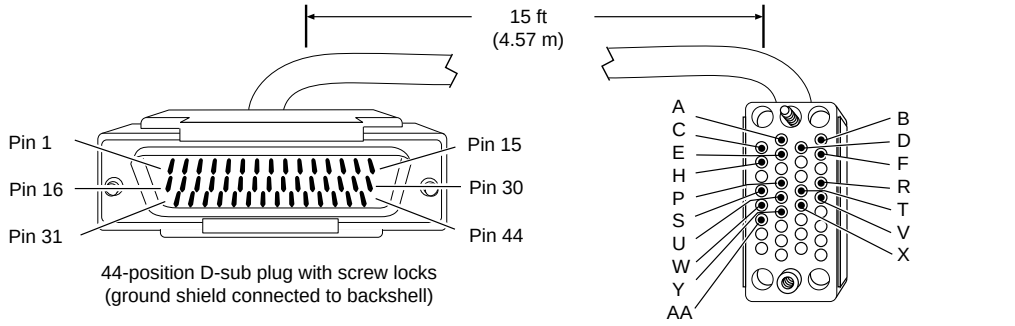
CAB0099A

Industry Interface Type: T1/DS1

Bay Networks Termination		**Remote Termination**
Signal	**Pin # to Pin #**	**Signal**
Transmit Tip	1 to 1	Transmit Tip
Transmit Ring	9 to 9	Transmit Ring
Receive Tip	3 to 3	Receive Tip
Receive Ring	11 to 11	Receive Ring
Ground	2 to 4	Ground*
Ground	4 to 2	Ground*

* You must configure onboard jumpers to complete this connection. Refer to the table called "QMCT1 Link Module Settings" in *Installing T1 Link Modules in BN Platforms*.

44-Pin to F V.35 Synchronous Pass-Through Cable (Order No. 7944)



44-position D-sub plug with screw locks
(ground shield connected to backshell)

34-position V.35 receptacle with screw jack retainers
(ground shield connected to backshell)

CAB0082A

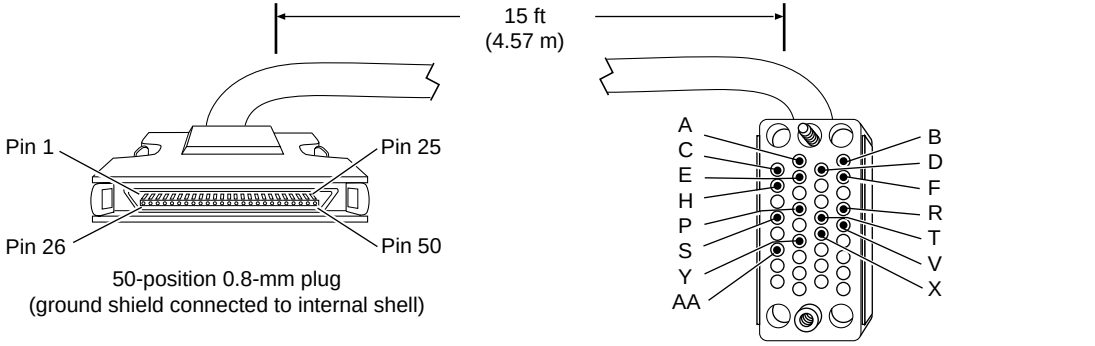
Industry Interface Type: V.35 (V.10 and V.11)

Bay Networks Termination		**Remote Termination**	
Signal	**Pin # to Pin #**		**Signal**
VSD +	38	R	Receive Data A
VSD -	36	T	Receive Data B
VRD +	37	P	Send Data A
VRD -	35	S	Send Data B
Request to Send +	4	F	Data Carrier Detect
Data Carrier Detect +	9	C	Request to Send
VTT +	40	Y	Send Timing A
VTT -	39	AA	Send Timing B
Frame Ground	1	A	Frame Ground
Signal Ground	7	B	Signal Ground
Internal Wire Connections			
Pin 4 > 5		Pin C > D	
Pin 32 > 34 > 40		Pin V > Y	
Pin 31 > 33 > 39		Pin X > AA	
Pin 13 > 28		Pin E > H	

(continued)

Bay Networks Termination	Remote Termination
Pin 14 > 29	
Pin 7 > 19 > 20 > 23 > 41 > 42	

50-Pin to F V.35 Synchronous Pass-Through Cable (Order No. 7946)



Industry Interface Type: V.35 (V.10 and V.11)

Bay Networks Termination		**Remote Termination**	
Signal	**Pin # to Pin #**		**Signal**
VSD +	44	R	Receive Data A
VSD -	19	T	Receive Data B
VRD +	43	P	Send Data A
VRD -	18	S	Send Data B
Request to Send +	4	F	Data Carrier Detect
Data Carrier Detect +	9	D	Clear to Send
VTT +	45	Y	Send Timing A
VTT -	20	AA	Send Timing B
Frame Ground	1	A	Frame Ground
Signal Ground	7	B	Signal Ground
Internal Wire Connections			
Pin 4 > 5		Pin C > D	
Pin 41 > 42 > 45		Pin V > Y	
Pin 16 > 17 > 20		Pin X > AA	
Pin 13 > 38		Pin E > H	
Pin 14 > 39			
Pin 7 > 30 > 31 > 34 > 46 > 47			

Configuring ATM Services

The following sections are ammendments to *Configuring ATM Services*:

- Change in ATM MAC Address Override Parameter Usage
- Defining Redundant LES/BUS Addresses
- LES/BUS Parameter Descriptions

Change in ATM MAC Address Override Parameter Usage

The ATM MAC Address Override parameter redefines the hardware MAC address for an ATM interface. Originally, this change took place only at the ATM layer to accommodate existing LAN emulation networks. For BayRS Version 12.10, the protocol layer also uses the MAC address override value. Upper-layer protocols (for example, IP or APPN) use this override value as the actual MAC address of the interface when sending packets.

For additional information about the ATM MAC Address Override parameter, see *Configuring ATM Services*.

Defining Redundant LES/BUS Addresses

BayRS Version 12.10/6.10 allows you to configure a prioritized list of up to four LAN emulation server/broadcast and unknown server (LES/BUS) addresses per LAN emulation client (LEC) or LAN emulation service record. You configure these addresses in the ATM LES List window (Figure 1).

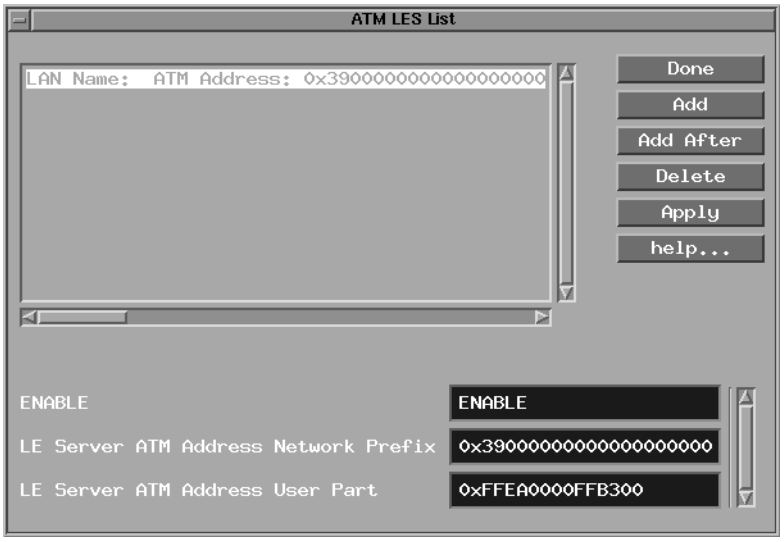


Figure 1. ATM LES List Window

After configuring the list of addresses, the LEC references the list and attempts to access the first LES/BUS address entry. If this attempt is unsuccessful, the LEC attempts to connect to the next LES/BUS address in the list. When the LEC reaches the last address in the list, it starts again at the beginning of the list until it successfully joins the emulated LAN.

Enabling a LES/BUS Entry

By default, you enable a LES/BUS entry when you add it to the service record. However, you can enable or disable a specific LES/BUS address at any time. Enable the LES/BUS entry to allow a LEC to access that address for information. Otherwise, disable the LES/BUS entry.

Entering a LES/BUS ATM Address

LE clients use the LAN emulation server (LES) to establish the control direct VCC. The LEC must know the LES address to obtain this information before it can join an emulated LAN. The LES/BUS address consists of a User Part and a Network Prefix.

If you select Manual configuration mode, you must configure at least one LES/BUS address. (See “Selecting a Configuration Mode” in Chapter 8 of *Configuring ATM Services*.) If you select Automatic configuration mode, you do not have to enter a LES/BUS address. The LE client receives the LES ATM address from the LAN emulation configuration server (LECS).

Adding a LES/BUS Address

You can add up to four LES/BUS addresses for each LAN emulation service record using the LANE Redundancy window (Figure 2).

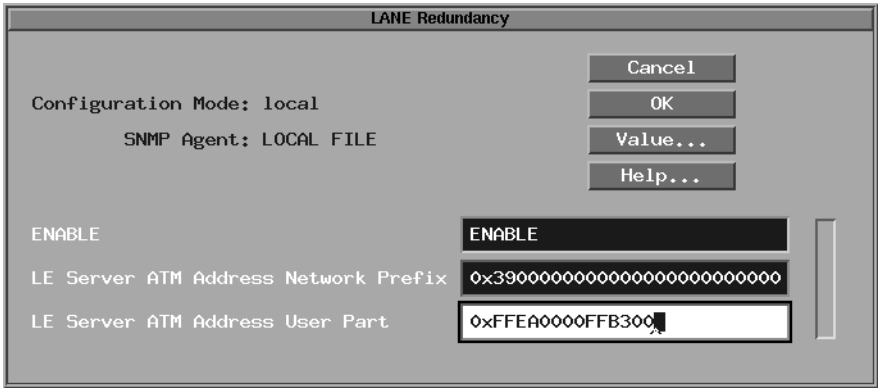


Figure 2. LANE Redundancy Window

To add a LES/BUS address:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on an interface configured for ATM.	The ATM Edit Connector window opens.
2. Click on **Service Attributes**.	The ATM Service Record List window opens.
3. Click on the desired LANE service record and then click on **LEC**.	The LAN Emulation Parameters window opens.
4. Change the **Configuration Mode** parameter to Manual	
5. Click on the desired LEC and then click on **LES**.	The ATM LES List window opens.
6. Click on **Add**.	The LANE Redundancy window opens.
7. Enter the LES address by setting values for the following parameters: • **LE Server ATM Address Network Prefix** • **LE Server ATM Address User Part** Click on **Help** or see the parameter descriptions beginning on page 16.	
8. Click on **OK**.	You return to the ATM LES List window.
9. Click on **Done**.	You return to the LAN Emulation Parameters window.
10. Click on **OK**.	You return to the ATM Service Record List window.
11. Click on **Done**.	You return to the Edit ATM Connector window.
12. Click on **Done**.	You return to the Configuration Manager window.

Inserting a LES/BUS Address out of Sequence

You can insert a LES/BUS address between two existing LES/BUS addresses by clicking on the Add After button in the ATM LES List window (see Figure 1). To use the Add After feature:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on an interface configured for ATM.	The Edit ATM Connector window opens.
2. Click on **Service Attributes**.	The ATM Service Record List window opens.
3. Click on the desired LANE service record and then click on **LEC**.	The LAN Emulation Parameters window opens.
4. Click on the desired LEC and then click on **LES**.	The ATM LES List window opens.
5. Click on the LES/BUS address in the list after which you want to add the new address.	The settings for this LES/BUS selection appear in the parameter boxes.
6. Click on **Add After**.	The LANE Redundancy window opens.
7. Enter the LES address by setting values for the following parameters: • **LE Server ATM Address Network Prefix** • **LE Server ATM Address User Part** Click on **Help** or see the parameter descriptions beginning on page16.	
8. Click on **OK**.	Site Manager adds the LES/BUS address and returns you to the ATM LES List window.
9. Click on **Done**.	You return to the LAN Emulation Parameters window.
10. Click on **OK**.	You return to the ATM Service Record List window.
11. Click on **Done**.	You return to the Edit ATM Connector window.
12. Click on **Done**.	You return to the Configuration Manager window.

Modifying a LES/BUS Entry

You can modify the parameters associated with a LES/BUS entry at any time. To modify a LES/BUS entry:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on an interface configured for ATM.	The Edit ATM Connector window opens.
2. Click on **Service Attributes**.	The ATM Service Record List window opens.
3. Click on the desired LANE service record and then click on **LEC**.	The LAN Emulation Parameters window opens.
4. Click on the desired LEC and then click on **LES**.	The ATM LES List window opens.
5. Click on the LES/BUS address you want to modify.	The settings for this LES/BUS selection appear in the parameter boxes.
6. Change the settings for one or more of the following parameters: • **Enable** • **LE Server ATM Address Network Prefix** • **LE Server ATM Address User Part** Click on **Help** or see the parameter descriptions beginning on page16.	
7. Click on **Apply**.	
8. Click on **Done**.	You return to the LAN Emulation Parameters window.
9. Click on **OK**.	You return to the ATM Service Record List window.
10. Click on **Done**.	You return to the Edit ATM Connector window.
11. Click on **Done**.	You return to the Configuration Manager window.

Deleting a LES/BUS Entry

To delete a LES/BUS address from the ATM LES List window:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on an interface configured for ATM.	The Edit ATM Connector window opens.
2. Click on **Service Attributes**.	The ATM Service Record List window opens.
3. Click on the desired LANE service record and then click on **LEC**.	The LAN Emulation Parameters window opens.
4. Click on the desired LEC and then click on **LES**.	The ATM LES List window opens.
5. Click on the LES/BUS address you want to delete.	The settings for this LES/BUS selection appear in the parameter boxes.
6. Click on **Delete**.	
7. Click on **Done**.	You return to the LAN Emulation Parameters window.
8. Click on **OK**.	You return to the ATM Service Record List window.
9. Click on **Done**.	You return to the Edit ATM Connector window.
10. Click on **Done**.	You return to the Configuration Manager window.

LES/BUS Parameter Descriptions

Parameter: **Enable**

Path: Configuration Manager > Protocols > ATM > Service Records > **LEC** > **LES**

Default: Enable

Options: Enable | Disable

Function: Enables or disables the chosen LAN emulation server (LES) on this service record.

Instructions: Accept the default, Enable, if you want the LAN emulation client to use this LES/BUS address in the specified order of preference. Select Disable if you do not want the LAN emulation client to consider this LES/BUS address.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.5.20.10.1.2

Parameter: **LE Server ATM Address Network Prefix**

Path: Configuration Manager > Protocols > ATM > Service Records > **LEC** > **LES**

Default: 39000000000000000000000000

Options: *XX*00000000000000000000000000 to *XX*FFFFFFFFFFFFFFFFFFFFFFFF

where XX = 39, 45, or 47

Function: Defines the network prefix of the ATM address for this LAN emulation server (LES). The network prefix specifies the ATM domain of which this LES is a part.

The *XX* byte must be 39, 45, or 47. This value defines the authority and format identifier (AFI). The AFI byte identifies the group responsible for allocating the prefix and the format the prefix uses. For more information about the AFI byte, see the ATM Forum UNI specification.

Instructions: If you want the LES to use the 39000000000000000000000000 network prefix, accept the default. If the LES resides in a different ATM domain, enter the network prefix for that domain.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.5.20.10.1.5

Parameter: **LE Server ATM Address User Part**

Path: Configuration Manager > Protocols > ATM > Service Records > **LEC** > **LES**

Default: None

Options: 00000000000000 to FFFFFFFFFFFFF

Function: Defines the user part (suffix) of the ATM address for a LAN emulation server (LES) on your network. The user part suffix consists of a 6-byte end-station identifier and a 1-byte selector field.

The user part and the network prefix form a complete ATM address.

Instructions: Enter the ATM address user part of the LES.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.5.20.10.1.5

Configuring BayStack Remote Access

Information in *Configuring BayStack Remote Access* is current for BayRS Version 12.00 and earlier. Most of the information in this guide has not changed with BayRS Version 12.10. However, be sure to see the following for the latest information:

For information on...	See this manual
Configuring an RMON data collection module (DCM)	*Configuring RMON and RMON2*
Configuring the startup option for an AN or ANH router	*Installing and Operating BayStack AN and ANH Routers*
Configuring the startup option for an ARN router	*Installing and Operating BayStack ARN Routers*

Configuring DECnet Services

The following section is an ammedment to *Configuring DECnet Services*.

Adjacent Host Address Parameter

The Destination Mac Address parameter, which appeared in the Static Adjacent Hosts List window, is renamed the Adjacent Host Address parameter. It supports an X.25 PVC logical channel number. See the following parameter description.

Parameter:	**Adjacent Host Address**
Path:	None
Default:	An empty list
Options:	Depends on the circuit type (see below)
Function:	Specifies the address of an adjacent host.
Instructions:	Enter the adjacent host address by following these guidelines: • If this circuit is not an X.25 PDN circuit, enter the 48-bit Ethernet address of the static adjacency. • If this circuit is an X.25 circuit that connects to an X.25 permanent virtual circuit (PVC), enter an X.25 logical channel number. • If this circuit is an X.25 circuit that connects to an X.25 switched virtual circuit (SVC), then enter a valid X.121 address.
MIB Object ID:	1.3.6.1.4.1.18.3.5.2.7.9

Configuring Dial Services

The following sections are amendments to *Configuring Dial Services*:

- Before You Begin
- Bandwidth-on-Demand Overview
- New Data Compression Protocol for all three Dial Services
- Bandwidth-on-Demand Congestion Monitor Parameters

Before You Begin

The last bulleted item in this section indicates that you should select router hardware modules if you open an existing configuration file in local mode. If this is an existing configuration file, the hardware is already defined.

Bandwidth-on-Demand Overview

In the Bandwidth-on-Demand overview in Chapter 2, there is a section entitled "Activating Dial-up Lines to Relieve Congestion," which describes how PPP multilink detects congestion. In the second paragraph, the sentence in parentheses should read: (Byte counts are measured after data compression).

New Data Compression Protocol for All Three Dial Services

Stac LZS is now available as a compression protocol for PPP circuits. Data compression can be used by all three dial services. To implement data compression, you must configure WCP or Stac LZS on a dial circuit.

For more information, refer to *Configuring Data Compression Services.*

Bandwidth-on-Demand Congestion Monitor Parameters

For BayRS 12.10, when WCP is negotiated above the multilink bundle and the router sends or receives data, it calculates the congestion thresholds based on compressed data. If WCP is negotiated below the bundle, the router calculates these thresholds based on uncompressed data.

If a router using software version 12.10 software is communicating with a router using software prior to version 12.10, the routers must negotiate WCP below the bundle, so the thresholds will be based on uncompressed data.

There are revisions for two of the congestion monitor parameters.

For the **BOD Full Threshold** parameter, the instructions should now read:

Enter a percentage that the router uses to measure congestion. If you configured the WAN compression protocol (WCP) on the circuit and it is configured to run below the multilink bundle, you may want to configure a threshold greater than 100 percent.

For the **BOD Recovery Threshold** parameter, the instructions should now read:

Enter a percentage that the router should reach before it returns to the leased line or bundle. If you configured the WAN compression protocol (WCP) on the circuit and it is configured to run below the multilink bundle, you may want to configure a threshold greater than 100 percent.

Configuring DLSw Services

The following topics describe amendments to *Configuring DLSw Services*:

Topic	Page
DLSw/APPN Boundary Function	20
IP Multicast Support for DLSw Version 2.0	30

DLSw/APPN Boundary Function

The *Data Link Switch* Version 2 (DLSw 2) is a mechanism for reliably transporting connection-oriented SNA and NetBIOS messages across an IP network. (Beginning with BayRS version 12.10, DLSw supports both IP unicast and IP multicast networks.)

Advanced Peer-to-Peer Networking (APPN) is an architectural extension of SNA. Bay Networks routers participate as APPN network nodes in an APPN network and communicate with adjacent network nodes and endnodes.

The *DLSw/APPN boundary function* (BF) allows DLSw to provide remote communications via an IP backbone and provide access over this backbone from enterprise-level applications using an APPN network.

The DLSw/APPN boundary function is implemented within a central APPN network node. The BF accepts traditional PU2 traffic supported by DLSW2 and routes it over APPN to the appropriate partner, typically a mainframe-based application.

DLSw/APPN Network Configurations

The DLSw/APPN boundary function can reside wherever your APPN backbone network is located.

In Figure 3, for example, the DLSw/APPN boundary function resides in an enterprise router located within the domain of the APPN mainframe or AS/400 data center. The corporate network is an IP network.

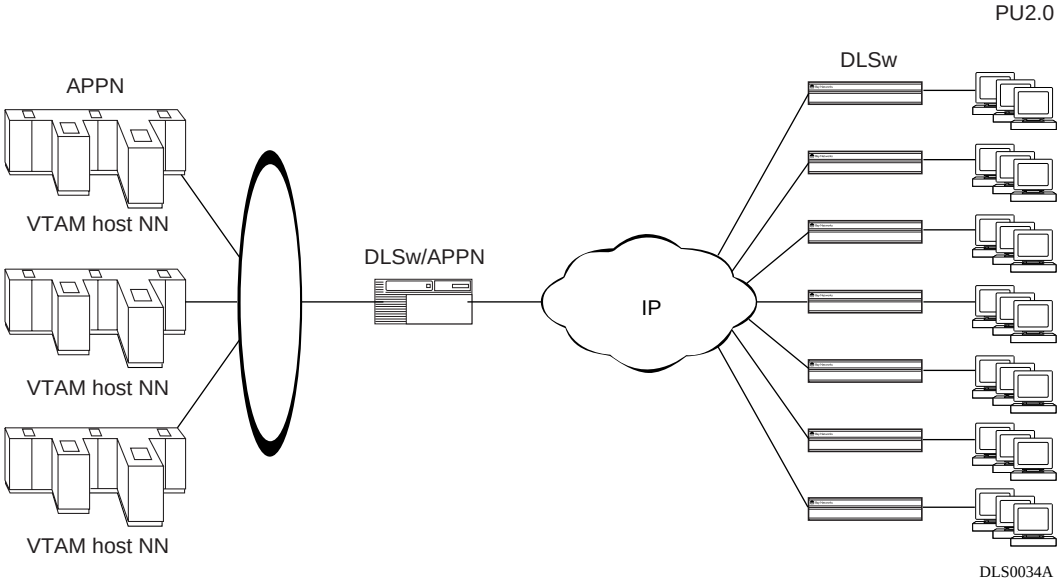


Figure 3. Data Center APPN Network

In Figure 4, the boundary function resides in a regional location. This enterprise-wide network has an APPN backbone. The regional location connects to the backbone through an IP network.

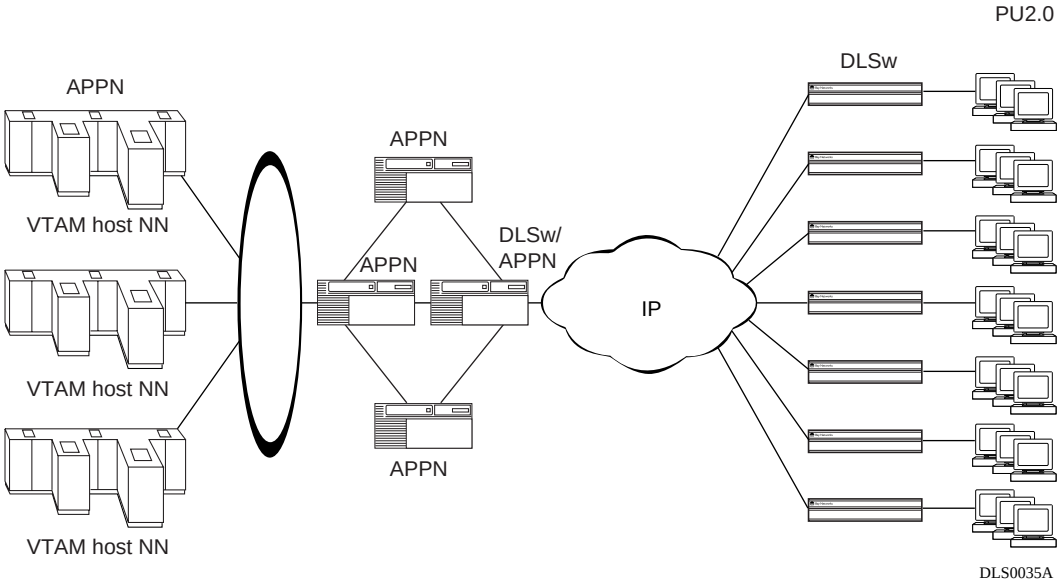


Figure 4. Enterprise APPN Network

DLSw/APPN Components

APPN and DLSw pass messages back and forth by means of a virtual circuit (VCCT) at the data link level. Figure 5 shows the relationship between APPN, DLSw, and the VCCT through which they exchange messages.

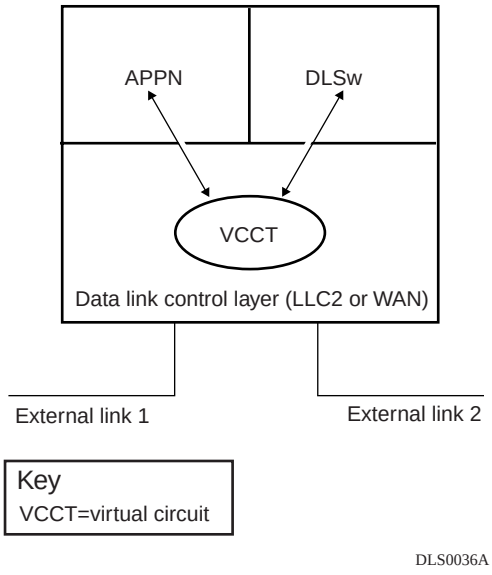


Figure 5. Boundary Function Virtual Circuit

APPN and DLSw send and receive messages on external links 1 and 2, and pass messages to each other through the virtual circuit.

The DLSw/APPN boundary function allows DLSw to provide remote communications via an IP backbone and provide access over this backbone from enterprise-level applications using an APPN network.

In Figure 6, Router 1 is running the DLSw/APPN boundary function. Router 2 is running DLSw only. The path between the host on Router 1 and the PU2.0 device on Router 2 passes through all the components involved in a communication between the host and the device. (DLUR, a component within APPN, is required because the 3174 system is configured as PU2.0.)

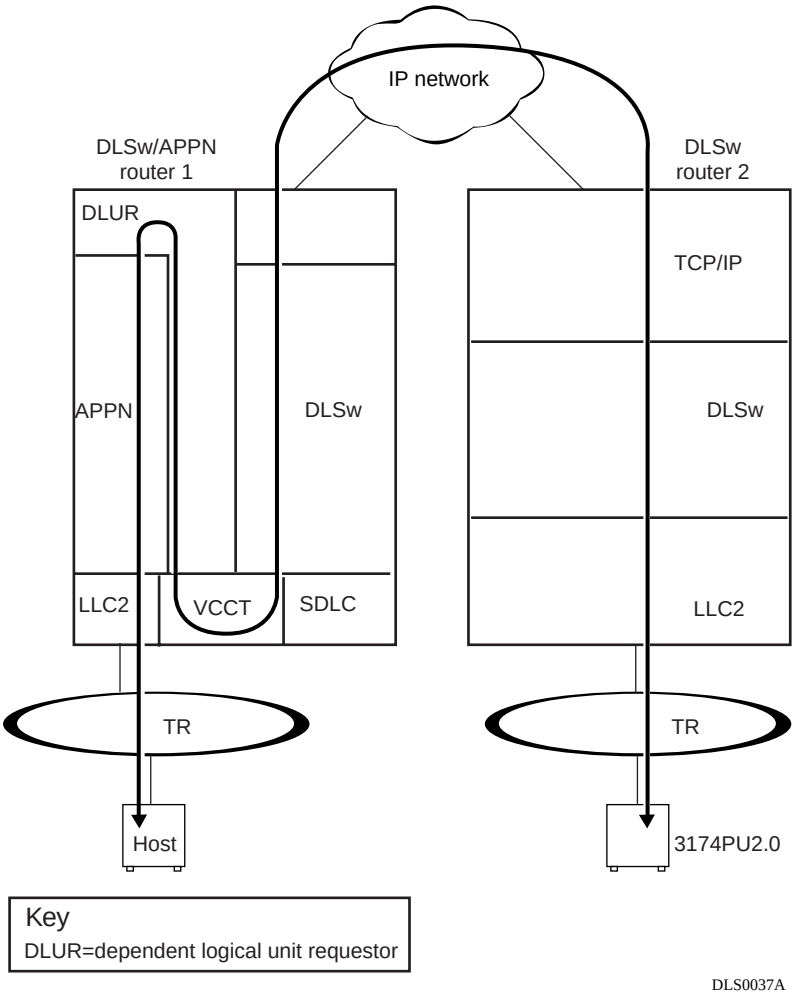


Figure 6. End-to-End Connection Using a DLSw/APPN Router and a DLSw Router

Configuring the DLSw/APPN Boundary Function

Instructions for configuring the DLSw/APPN boundary function are covered in this manual under the following topics:

Topic	Page
Step 1: Configuring DLSw and APPN	25
Step 2: Creating a Virtual Circuit and Adding a DLSw Interface	26
Step 3: Obtaining the Virtual Circuit Number	27
Step 4: Adding an APPN Interface to an Existing Virtual Circuit	28
Disabling and Reenabling the Boundary Function	29

Step 1: Configuring DLSw and APPN

Before you can configure the DLSw boundary function, DLSw and APPN must be running on the same slot on the router. Using Site Manager:

1. **Configure DLSw on a slot.**

   For instructions, see *Configuring DLSw Services*.

2. **Configure APPN on the same slot as DLSw.**

   You must supply information for the following APPN advanced global parameters:

   - Default DLUS Name
   - Default Backup DLUS Name

   Set the Max Send BTU Size and Max Receive BTU Size APPN advanced port parameters. Set these parameters according to the size supported by the end device. If you enable HPR support, set these parameters to 768 or greater

   The DLSw/APPN boundary function requires a setting of Enable for the Implicit DLUR parameter. When you configure the DLSw/APPN boundary function, Site Manager automatically sets the Implicit DLUR parameter to Enable. Make sure that this parameter is properly set.

   For information on configuring APPN, see *Configuring APPN Services.*

Step 2: Creating a Virtual Circuit and Adding a DLSw Interface

Begin at the Configuration Manager window:

1. **Click on Protocols.**

   The protocols menu opens.

2. **Click on DLSw.**

   The DLSw window opens.

3. **Click on Boundary Function.**

   The Boundary Function window opens.

4. **Click on Add VCCT.**

   Site Manager asks: “Do you want to create a new Virtual Circuit or use an existing one?”

5. **Click on OK to create a new virtual circuit and add a DLSw interface to the virtual circuit.**

   The VCCT Slot Configuration window opens.

6. **Specify a slot for virtual circuit you are creating.**

   The slot you choose for the virtual circuit must be the same slot on which DLSw and APPN are running.

7. **Click on OK.**

   Site Manager returns you to the Configuration Manager window.

You have now created a virtual circuit and added a DLSw interface to the circuit.

To configure the DLSw/APPN boundary function, you must now add an APPN interface to the same virtual circuit as described in “Step 4: Adding an APPN Interface to an Existing Virtual Circuit” on page 28.

Step 3: Obtaining the Virtual Circuit Number

Site Manager assigns a circuit number to each virtual circuit you create. When you add an APPN interface to the virtual circuit you are using to support the boundary function, you must specify the circuit number assigned to the VCCT. To obtain this information:

1. **Click on Protocols.**

   The protocols menu opens.

2. **Click on Global Protocols.**

   The the Global Protocols window opens.

3. **Click on VCCT.**

   The VCCT menu opens.

4. **Click on Interfaces.**

   The VCCT circuits window opens, listing all the virtual circuits on the router. Each entry specifies the slot and circuit number of the virtual circuit.

5. **Make a note of the circuit number of the VCCT you have created and click on Done.**

   Site Manager returns you to the Configuration Manager window.

Step 4: Adding an APPN Interface to an Existing Virtual Circuit

Begin at the Configuration Manager window:

1. **Click on Protocols.**

   The protocols menu opens.

2. **Click on APPN.**

   The APPN window opens.

3. **Click on Boundary Function.**

   The Boundary Function window opens.

4. **Click on Add VCCT.**

   Site Manager asks: “Do you want to create a new Virtual Circuit or use an existing one?”

5. **Click on Cancel to use an existing virtual circuit.**

   The VCCT CCT Configuration window opens.

6. **Supply the slot and circuit number of the virtual circuit to which you want to add an APPN interface.**

7. **Click on Done.**

   The APPN configuration window opens.

8. **Supply a MAC address and a SAP for the interface, as described in *Configuring APPN Services*.**

9. **Click on Done.**

   Site Manager asks: “Would you like to configure Adjacent Link Stations on this port?”

10. **Click on Cancel.**

    Site Manager returns you to the Configuration Manager window.

Disabling and Reenabling the Boundary Function

By default, the DLSw/APPN boundary is enabled on the router. You can use the following Site Manager procedure to disable and reenable it.

Site Manager Path	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **DLSw**.	The DLSw menu opens.
3. Choose **Boundary Function**.	The Boundary Function menu opens.
4. Choose **Global**.	The Edit VCCT Global Parameters window opens.
5. Set the **Enable** parameter.	
6. Click on **OK**.	Site Manager returns you to the Configuration Manager window.

IP Multicast Support for DLSw Version 2.0

This section describes BayRS version 12.10 multicast enhancements to data link switching (DLSw) services. For complete information about DLSw, see *Configuring DLSw Services.*

Topic	Page
Configuring DLSw in RFC 2166 Multicast Mode	30
Configuring IP Multicast Protocols on the Router	31
Assigning an IP Multicast Group Address to a Slot	31
Sample Connection Using DLSw and IP Multicasting	34
Using Site Manager to Configure DLSw for IP Multicasting	35

Configuring DLSw in RFC 2166 Multicast Mode

Beginning with version 12.10 of the BayRS software, DLSw provides IP multicast support in addition to IP unicast broadcast services. The capability to send and receive both IP multicast traffic and IP unicast traffic makes the Bay Networks implementation of DLSw fully compliant with RFC 2166.

RFC 2166 reduces the amount of broadcast traffic on the network. A comparison of RFC 2166 with earlier DLSw RFCs 1434 and 1795 shows how this happens:

- Under RFCs 1434 and 1795, an endstation (an SNA or NetBIOS application) that wants to establish a network connection first sends a DLSw SSP CanuReach (or NETBIOS_NQ) message to all routers that are part of the DLSw network. In a large network with many endstations, these connection attempts result in a large number of packets traveling on the network. In addition, under RFCs 1434 and 1795, TCP connections must be constantly maintained between all participating routers within the DLSw network.
- Under RFC 2166, network connections are established only when needed and maintained only as long the endstations require. In addition, endstations use multicast IP to send the initial CanuReach (or NET_BIOS) messages, thus reducing the amount of traffic on the network.

By default, DLSw operates in RFC 1434 mode. You can use Site Manager to configure DLSw in RFC 2166 multicast mode. For instructions, see "Using Site Manager to Configure DLSw for IP Multicasting" on page 35.

Configuring IP Multicast Protocols on the Router

A router configured for DLSw with IP multicasting support must also be running:

- IP
- IGMP
- DVMRP, MOSPF, or both

You must configure IP on at least one slot on the router and assign an IP address to each DLSw slot as described in *Configuring DLSw Services.*

For complete information about IP multicasting and instructions for configuring IGMP, DVMRP, and MOSPF on the router, see *Configuring IP Multicasting and Multimedia Services*.

Assigning an IP Multicast Group Address to a Slot

In an IP multicasting network, a sender -- or *source* -- of IP multicast datagrams addresses each datagram to a *group* of receivers. An IP multicast group address is a Class D address (the high order bits are set to 1110) from 224.0.0.0 to 239.255.255.255.

On a router configured for DLSw multicasting, each DLSw slot is associated with an IP multicast group address. The router in Figure 7, for example, is running DLSw on slot 3. The network administrator has assigned the group address 224.0.10.0 to slot 3.

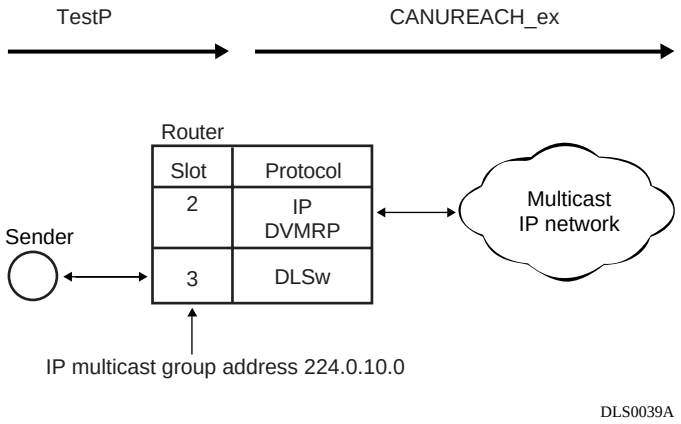


Figure 7. Addressing a Message to an IP Multicast Group

When DLSw receives a TestP message, the following steps occur:

1. DLSw converts the TestP message into a CANUREACH_ex message.
2. DLSw uses the IP multicast group address associated with slot 3 -- 224.0.10.0 -- as the destination address of the CANUREACH message.
3. DLSw passes the message to IP running on slot 2.
4. IP sends the message to the IP multicast network.

When the router receives a CANUREACH_ex message on a slot configured with IP, the reverse sequence occurs (see Figure 8):

1. The router receives a CANUREACH_ex message.
2. IP determines that the CANUREACH_ex message is addressed to multicast group 224.0.10.0.
3. IP forwards the message to DLSw on slot 3.
4. DLSw converts the CANUREACH_ex message to a TestP message and sends it out a DLSw interface to the receiver.

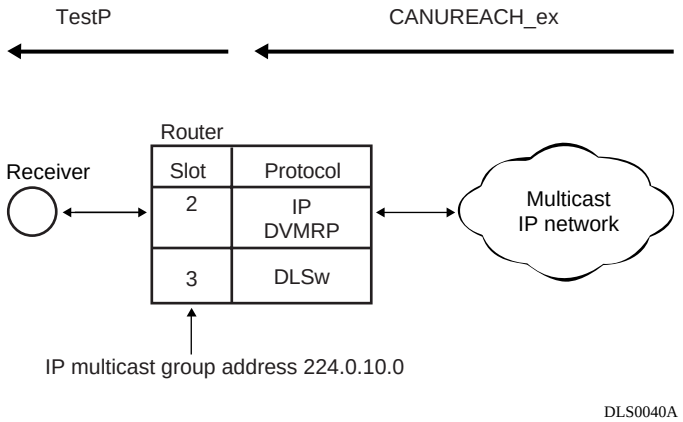


Figure 8. Receiving a Message Addressed to a Multicast Group

You can use Site Manager to specify an IP multicast group address and associate it with a DLSw slot or slots. For instructions, see "Using Site Manager to Configure DLSw for IP Multicasting" on page 35.

Sample Connection Using DLSw and IP Multicasting

Figure 9 shows a pair of routers running DLSw in RFC 2166 mode. On Router A, IP and DVMRP are running on slot 2, and DLSw is running on slot 3. On Router B, DLSw is running on slot 2, and IP and DVMRP are running on slot 3.

Router A connects to Endstation 1 through a DLSw interface on slot 3. Router A has an IP interface on slot 2 to the IP multicast network. Routers B and C are configured identically. Both connect to hosts through a DLSw interface on slot 2. Both have an interface to the IP network on slot 3.

On Router A, the network administrator has assigned IP multicast group address 224.0.10.0 to DLSw slot 3. On Router B, the network administrator has assigned group address 224.0.10.0 to DLSw slot 2

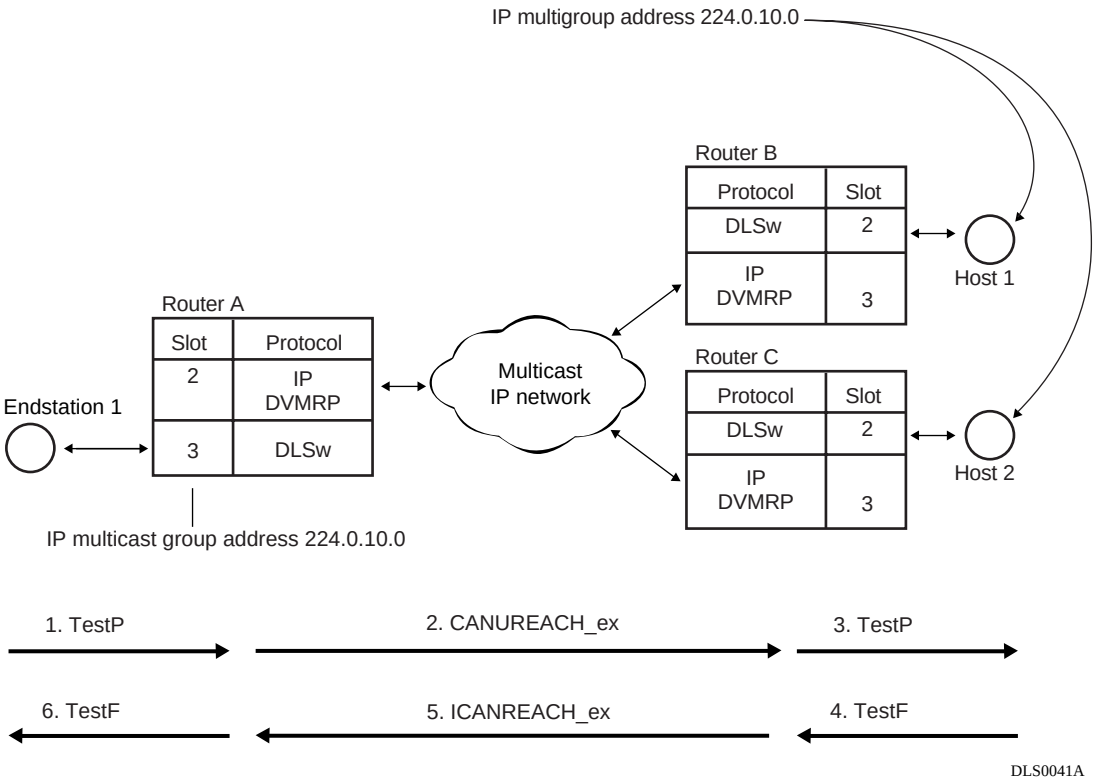


Figure 9. Multicast DLSw

When Endstation 1 generates an SNA TestP message, the following steps occur:

1. Router A receives the TestP message on slot 3.
2. Router A multicasts a CANUREACH_ex message on slot 2, using the group address 224.0.10.0.
3. Router B receives the CANUREACH_ex message and forwards the message to slot 3, configured with the IP multicast group address.
4. Router B sends a TestP (or NameQuery) message on slot 3 to Host 1.
5. Host 1 responds to the TestP message by sending a TestF message.
6. Router B receives the TestF message on slot 3.
7. Router B sends an ICANREACH_ex message on slot 2. (Router B sends this message in an IP unicast datagram, as described in *Configuring DLSw Services*.)
8. Router A receives the ICANREACH_ex unicast message on slot 2 and forwards it to DLSw slot 3.
9. Router A sends a TestF message to Endstation 1.

Using Site Manager to Configure DLSw for IP Multicasting

To configure DLSw for IP multicasting, you must:

- Configure DLSw to run in RFC 2166 multicast mode.
- Enable IGMP.
- Supply an IP multicast group address and assign the address to a DLSw slot.

The following Site Manager procedure shows you how to add DLSw IP multicast support to a router that is already running DLSw:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **DLSw.**	The DLSw menu opens.
3. Choose **Basic Global**.	The DLSw Basic Global Parameter window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
4. Click on the **DLSw RFC Version** parameter. Click on the **Values** button.	The Values window opens.
5. Click on **RFC2166 (Multicast)**. Click on **OK**.	The Initial IGMP Global Configuration window opens (if IGMP is not configured).
6. Set IGMP global parameters (or accept the defaults) and click on **Save**.	The DLSw Multicast Configuration window opens.
7. Click on **Add**.	A second DLSw Multicast Configuration window opens.
8. Supply an IP multicast group address and associate the address with a slot or slots. Click on **OK**.	The first DLSw Multicast Configuration window reopens.
9. Click on **Done**.	The Configuration Manager window opens.

Configuring Ethernet, FDDI, and Token Ring Services

The following section is an ammendment to *Configuring Ethernet, FDDI, and Token Ring Services*.

CSMA/CD Line Parameters

Use the following two parameters when you configure Ethernet line services on a 100Base-T module:

Parameter: Interface Line Speed

Path: Configuration Manager > **XCVR** Connector (100Base-T only) > **Edit Line** > Edit CSMA/CD Parameters

Default: 100Base-TX/100Base-FX (for 100Base-FX Ethernet modules);
Auto Negotiation (for 10/100Base-TX Ethernet modules)

Options: Auto Negotiation │ 10Base-T │ 10Base-T (Full Duplex) │ 100Base-TX/100Base-FX │ 100Base-TX (Full Duplex)

Note: The options that are available differ, depending on the module you are using.

Function: Specifies the configured line speed and duplex setting for the selected interface, or enables automatic line negotiation.

Instructions: To enable automatic line negotiation, select Auto Negotiation.

To configure a specific line speed, select one of the following:

- 10Base-T
- 10Base-T (full Duplex)
- 100Base-TX/100Base-FX
- 100Base-TX (full duplex)

Selecting a specific line-speed configuration disables Auto Negotiation.

MIB Object ID: 1.3.6.1.4.1.18.3.4.16.1.1.4

Parameter: **Line Advertising Capabilities**

Path: Configuration Manager > **XCVR** Connector (100Base-T only) > **Edit Line** > Edit CSMA/CD Parameters > Interface Line Speed parameter = Auto Negotiation > **OK** > **Configure Line Capabilities** > Line Advertising Capabilities

Default: 1111

Options: 0000 | 1000 | 0100 | 0010 | 0001 | 1111

Function: Specifies the line configurations available to remote nodes that have automatic line negotiation capability.

Instructions: Select the code for the desired line advertising:

- No advertising = 0000
- 10Base-T = 1000
- 10Base-T, full duplex only = 0100
- 100Base-TX, = 0010
- 100Base-TX, full duplex only = 0001
- All advertising = 1111

MIB Object ID: 1.3.6.1.4.1.18.3.4.16.1.1.9

Configuring IP Multicasting and Multimedia Services

The following sections are ammendments to *Configuring IP Multicasting and Multimedia Services*:

- Guidelines for Configuring IP Multicasting and Multimedia Services
- Configuring IP Multicasting and Multimedia Services with Site Manager

Guidelines for Configuring IP Multicasting and Multimedia Services

The following sections supplement the instructions in *Configuring IP Multicasting and Multimedia Services*:

- Configuring MOSPF, QOSPF, and DVMRP
- Monitoring MOSPF
- Monitoring DVMRP
- Configuring the Expanding Ring Search

- Configuring Administratively Scoped Multicast
- Configuring the Static Forwarding Entry
- Configuring the DVMRP Prune Lifetime
- Configuring Multicasting Policies

Configuring MOSPF, QOSPF, and DVMRP

Version 12.10 does not support dynamic configuration of MOSPF/QOSPF. After making local configuration changes, restart OSPF by disabling and reenabling it.

Version 12.10 QOSPF supports inter-area and intra-area multicast only with RSVP FF reservation style.

If you enable MOSPF, do not run other multicasting protocols on any OSPF interfaces, even if MOSPF is disabled on those interfaces (that is, even if you set the Multicast Forwarding parameter to blocked).

If you want to disable MOSPF on a network, use Site Manager to disable MOSPF on all routers in the network. See *Configuring IP Multicasting and Multimedia Services*, "Configuring Multicast Forwarding on an OSPF Interface."

If you are configuring a network with both MOSPF and non-MOSPF routers, set all non-MOSPF routers to priority 0 so that the MOSPF routers can become DR/BDR, which is necessary for MOSPF to work.

If the network contains any routers running versions earlier than 12.10, and you configure a Version 1210 router to advertise DVMRP routes into an MOSPF domain, configure it to originate AS external link advertisements for both unicast and multicast routes (that is, use the same entry point for both external unicast and external multicast routes).

Version 12.10 supports only the ignore action of the DVMRP announce route policy. It does not support a DVMRP accept route policy.

Version 12.10 does not support an MOSPF accept route policy. Use the MOSPF announce route policy to import DVMRP routes as multicast ASE routes. When connecting an MOSPF domain to an MBONE implementation via a DVMRP, keep the OSPF database small by configuring the MOSPF route announce policy to import only the default DVMRP route to the MOSPF domain.

Note: Refer to the *Release Notes for Site Manager Software Version 6.10* to configure the DVMRP, MOSPF, IGMP, and MTM policy filter parameters.

We recommend that you avoid using MOSPF in a transit domain for multicast.

The router will time out an MOSPF forwarding entry a certain time after it receives the last packet in the flow. The default timeout value is 600 seconds. You can change this value by setting the Timeout Value parameter. To access this parameter, begin at the Configuration Manager window and click on Protocols, IP, OSPF, and Global. If most flows are short-lived, set the value to a number that slightly exceeds the interval between two packets of the same flow. For example, if you expect the longest interval between two packets of a flow to be 1 minute, set the timeout value to 90 seconds. Setting the value below the interval is acceptable but it does cause unnecessary Dijkstra.

Monitoring MOSPF

On a router running both MOSPF and DVMRP, the following values indicate an external upstream interface (that is, a DVMRP interface):

- The `Upstream Interface` value `255.255.255.254` appears when you enter the Technician Interface **show mospf fwd** command.
- The `in` value `-2` appears when you enter the Technician Interface **ip mospf_fwd** command.

Monitoring DVMRP

The dvmrp.bat script has changed as follows because DVMRP no longer forwards data:

- The Technician Interface does not display In Drops and Out Drops statistics in response to the **show dvmrp stats circuits** command.
- The Technician Interface does not display In Packets, Out Packets, Ip Drop, Out Drop, and Thrshld Drop statistics in response to the **show dvmrp stats vifs** command.

Configuring the Expanding Ring Search

The support for Expanding Ring Search in MOSPF is disabled by default for better performance. You can use Site Manager to enable it. See *Configuring IP Multicasting and Multimedia Services*, "Enabling Dynamic TTL."

Configuring Administratively Scoped Multicast

Packets with administratively scoped multicast addresses are locally assigned and are not required to be unique across administrative boundaries because they do not cross them. Refer to the Internet Draft *Administratively Scoped IP Multicast* (draft-ietf-mboned-admin-ip-space-03.txt) for details.

Version 12.10 does not support the dynamic configuration of administratively scoped multicast. Site Manager also does not support it. Use the Technician Interface to configure it via the wfIgmpBoundaryEntry MIB object.

Configuring the Static Forwarding Entry

Version 12.10 does not support the dynamic configuration of the multicast Static Forwarding Entry. Refer to "MTM Static Forwarding Policy Parameters" in the *Release Notes for Site Manager Software Version 6.10* to control the forwarding of multicast packets.

Static forwarding entries statically determine how the router forwards particular multicast flows. You cannot use both static and dynamic (via multicast protocols) forwarding. For example, you cannot configure a static forwarding entry to specify that for a particular source/group pair, the router accept packets on Circuit 1, forward them out Circuits 2 and 3, but rely on a multicast protocol to dynamically decide if those packets should be forwarded out Circuit 4.

Configuring the DVMRP Prune Lifetime

By default, DVMRP sets a lifetime of 7200 seconds on the prune messages it sends out an interface. You can use Site Manager to specify a lifetime between 0 and 86,400 seconds.

Beginning at the Configuration Manager window, click on Protocols and IP. The IP protocol menu appears. Click on Multicast, DVMRP, and Circuit. The DVMRP circuit window opens. Set the Prune Life Time parameter and click on Done.

Configuring Multicasting Policies

You can use Site Manager to configure routing policies for DVMRP, MOSPF, IGMP, and MTM.

Beginning at the Configuration Manager, click on Protocols and IP. The IP protocol menu appears. Click on Policy Filters and select the multicasting protocol for which you want to configure a policy. A protocol-specific window for the policy opens. Set the parameters to define the policy and click on Done.

Configuring IP Multicasting and Multimedia Services with Site Manager

This section supplements Appendix A, "Site Manager Parameters," in *Configuring IP Multicasting and Multimedia Services*. It provides the Site Manager menu path to each DVMRP, MOSPF, IGMP, and MTM policy filter parameter, information about default settings, valid parameter options, the parameter function, instructions for setting the parameter, and the MIB object ID.

Note: The following DVMRP, MOSPF, and IGMP policy filter parameter descriptions provide more detailed descriptions than the parameter online Help. Parameter online Help is not available for the MTM policy filter parameters. Use the descriptions in "MTM Static Forwarding Policy Parameters" on page 52 instead.

Announce Policy Parameters for Both DVMRP and MOSPF

Use the following descriptions to set DVMRP and MOSPF announce policies.

Parameter: Enable

Path: Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Announce Policies

Path: Configuration Manager > Protocols > IP > Policy Filters > MOSPF > Announce Policies

Parameter:	**Enable**
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables this policy.
Instructions:	Set to Disable to disable the policy.
MIB Object ID:	DVMRP: 1.3.6.1.4.1.18.3.5.3.2.6.16.1.2
MIB Object ID:	MOSPF: 1.3.6.1.4.1.18.3.5.3.2.6.14.1.2

Parameter:	**Name**
Path:	Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Announce Policies
Path:	Configuration Manager > Protocols > IP > Policy Filters > MOSPF > Announce Policies
Default:	None
Options:	Any alphanumeric character string
Function:	Identifies this policy.
Instructions:	Enter a unique name for the policy.
MIB Object ID:	DVMRP: 1.3.6.1.4.1.18.3.5.3.2.6.16.1.4
MIB Object ID:	MOSPF: 1.3.6.1.4.1.18.3.5.3.2.6.14.1.4

Parameter: **Networks**

Path: Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Announce Policies

Path: Configuration Manager > Protocols > IP > Policy Filters > MOSPF > Announce Policies

Default: An empty list

Options: A list of network identifiers. Each identifier consists of a network number, a mask, and a flag to indicate whether the ID refers to a specific network or a range of networks.

Function: Specifies which networks will match this policy.

Instructions: Enter a specific encoding of 0.0.0.0/0.0.0.0 to match the default route. Enter a range encoding of 0.0.0.0/0.0.0.0 to match any route. Enter an empty list to match any route.

MIB Object ID: DVMRP: 1.3.6.1.4.1.18.3.5.3.2.6.16.1.5

MIB Object ID: MOSPF: 1.3.6.1.4.1.18.3.5.3.2.6.14.1.5

Parameter: **Action**

Path: Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Announce Policies

Path: Configuration Manager > Protocols > IP > Policy Filters > MOSPF > Announce Policies

Default: DVMRP: Ignore

MOSPF: Announce

Options: DVMRP: Ignore

MOSPF: Announce | Ignore

Function: Specifies whether to advertise a route that matches this policy.

Instructions: DVMRP: Ignore is the only option available. The router drops the route.

MOSPF: To advertise the route, specify Announce. To drop the route, specify Ignore.

MIB Object ID: DVMRP: 1.3.6.1.4.1.18.3.5.3.2.6.16.1.6

MIB Object ID: MOSPF: 1.3.6.1.4.1.18.3.5.3.2.6.14.1.6

Parameter:	**Rule Precedence** or **Precedence**
Path:	Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Announce Policies
Path:	Configuration Manager > Protocols > IP > Policy Filters > MOSPF > Announce Policies
Default:	0
Options:	A metric value
Function:	Specifies a metric value to be used to compare this policy with other policies that a route may match. A policy with a higher metric takes precedence over a policy with a lower metric. In case of a tie, the protocol uses an internal index value assigned to the policy by IP software. The position of the policy in the list indicates the index value from lowest to highest.
Instructions:	Use this parameter to assign precedence to policies that match the same route.
MIB Object ID:	DVMRP: 1.3.6.1.4.1.18.3.5.3.2.6.16.1.7
MIB Object ID:	MOSPF: 1.3.6.1.4.1.18.3.5.3.2.6.14.1.7

Parameter:	**Advertise**
Path:	Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Announce Policies
Path:	Configuration Manager > Protocols > IP > Policy Filters > MOSPF > Announce Policies
Default:	An empty list
Options:	A list of network identifiers
Function:	Specifies network IDs to include in place of the network IDs listed in the route to be advertised.
Instructions:	Specify a non-null value only if the announce Action parameter is Propagate. The values you enter in the advertise list determine the action taken. If you supply a list of network IDs, these IDs are advertised instead of the actual IDs in the route. If you use the default (an empty list), the actual IDs are advertised. Note that by default, BGP-4 aggregates subnets into their natural network IDs. If you supply a list that includes the encoding 255.255.255.255/ 255.255.255.255, the actual network IDs are advertised along with the other IDs in the advertise list. This allows advertisement of an aggregate or default along with the actual network. If the actual network is a subnet (and the advertising protocol supports subnet advertisements), the subnet is advertised.
MIB Object ID:	DVMRP: 1.3.6.1.4.1.18.3.5.3.2.6.16.1.10
MIB Object ID:	MOSPF: 1.3.6.1.4.1.18.3.5.3.2.6.14.1.10

DVMRP-Specific Announce Policy Parameters

Use the following descriptions to set DVMRP-specific announce policies.

Parameter: Filtered Circuits

Path: Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Announce Policies

Default: An empty list

Options: Leave empty or specify one or more 2-octet circuit numbers.

Function: This is a list of DVMRP circuits. By specifying a circuit in this list, the filter applies to DVMRP advertisements sent using that circuit.

Instructions: If you want this filter to apply to any outbound DVMRP circuit, do not specify any value for this parameter.

If you want this filter to apply to specific outbound DVMRP circuits, specify the circuit numbers in 2-octet strings.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.16.1.22

Parameter: Filtered Tunnels

Path: Configuration Manager > Protocols > IP > Policy Filters > DVMRP > Announce Policies

Default: An empty list

Options: Leave empty or specify one or more 8-octet IP addresses.

Function: This is a list of DVMRP tunnels. If a tunnel interface appears in this list the filter applies to DVMRP advertisements sent via that tunnel. Each tunnel takes 8 octets, the first 4 of which are for the local IP address and the last 4 are for the remote IP address.

Instructions: If you want this filter to apply to any DVMRP tunnel, do not specify any value for this parameter.

If you want this filter to apply to specific DVMRP tunnels, specify the IP addresses in 8-octet strings. Entering all Fs for the first IP address turns off this filter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.16.1.23

IGMP Group Policy Parameters

Use the following descriptions to set IGMP group policies.

Parameter: Enable

Path:	Configuration Manager > Protocols > IP > Policy Filters > IGMP
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables this policy.
Instructions:	Set this parameter as required.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.6.11.1.2

Parameter: Name

Path:	Configuration Manager > Protocols > IP > Policy Filters > IGMP
Default:	None
Options:	Any alphanumeric character string
Function:	Specifies a user name for this policy.
Instructions:	Enter a unique name for this policy.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.6.11.1.4

Parameter: **Sources**

Path: Configuration Manager > Protocols > IP > Policy Filters > IGMP

Default: An empty list

Options: Leave empty or specify one or more sources.

Function: Identifies which sources will match this rule.

Instructions: If you want this filter to match any source, do not specify any value for this parameter.

To specify an exact source address or range of source addresses, enter one or more octet groupings in the following form:

First octet: exact (1) or range (2)

Next 4 octets: source address

Next 4 octets: source mask

An entry with an exact tag matches only the specific source (number and mask). An entry with a range tag matches any prefix that falls in the range indicated by the source and mask.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.11.1.5

Parameter: **Action**

Path: Configuration Manager > Protocols > IP > Policy Filters > IGMP

Default: Ignore

Options: Accept │ Ignore

Function: Specifies whether to accept or ignore the group join.

Instructions: Specify Accept to accept the group join, or Ignore to ignore the group join.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.11.1.6

Parameter: Precedence

Path:	Configuration Manager > Protocols > IP > Policy Filters > IGMP
Default:	0
Options:	A metric value
Function:	Specifies a metric value to be used to compare this policy with other policies that a route may match. A policy with a higher metric takes precedence over a policy with a lower metric. In case of a tie, the protocol uses an internal index value assigned to the policy by IP software. The position of the policy in the list indicates the index value from lowest to highest.
Instructions:	Use this parameter to assign precedence to policies that match the same route.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.6.11.1.8

Parameter: Groups

Path:	Configuration Manager > Protocols > IP > Policy Filters > IGMP
Default:	An empty list
Options:	Leave empty or specify one or more groups.
Function:	Identifies which groups match this rule.
Instructions:	If you want this filter to match any group, do not specify any value for this parameter. To match specific groups, enter group number and group mask combinations as follows: First 4 octets: group number Next 4 octets: group mask
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.6.11.1.10

Parameter: Circuits

Path:	Configuration Manager > Protocols > IP > Policy Filters > IGMP
Default:	An empty list
Options:	Leave empty or specify one or more 2-octet circuit numbers.
Function:	Identifies which circuits match this rule.
Instructions:	If you want this filter to match any circuit, do not specify any value for this parameter. If you want this filter to apply to specific circuits, enter the circuit numbers in 2-octet strings.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.6.11.1.11

Parameter: Senders

Path:	Configuration Manager > Protocols > IP > Policy Filters > IGMP
Default:	An empty list
Options:	Leave empty or specify one or more sender address and sender mask octet combinations.
Function:	Identifies which senders match this rule.
Instructions:	If you want this filter to match any sender, do not specify any value for this parameter. To match specific senders, enter sender address and sender mask combinations as follows: First 4 octets: sender address Next 4 octets: sender mask
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.6.11.1.12

MTM Static Forwarding Policy Parameters

Use the following descriptions to set MTM static forwarding policies.

Parameter: Enable

Path:	Configuration Manager > Protocols > IP > Policy Filters > MTM
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables this policy.
Instructions:	Set to Disable to disable the policy.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.6.12.1.2

Parameter: Name

Path:	Configuration Manager > Protocols > IP > Policy Filters > MTM
Default:	None
Options:	Any alphanumeric character string
Function:	Identifies this policy.
Instructions:	Enter a unique name for the policy.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.6.12.1.4

Parameter: Groups

Path:	Configuration Manager > Protocols > IP > Policy Filters > MTM
Default:	An empty list
Options:	Leave empty or specify one or more groups.
Function:	Identifies which groups match this rule.
Instructions:	If you want this filter to match any group, do not specify any value for this parameter. To match specific groups, enter group number and group mask combinations as follows: First 4 octets: group number Next 4 octets: group mask
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.6.12.1.5

Parameter: Preference

Path: Configuration Manager > Protocols > IP > Policy Filters > MTM

Default: 1

Options: 0 | any integer from 1 to 16

Function: Accept the default (1) setting or assign a nonzero value (from 1 to 16) if you want the policy to overwrite multicast protocols. Specify 0 if you want multicast protocols to overwrite the policy.

If the policy can overwrite protocols, it makes the forwarding decisions. If protocols can overwrite the policy, the protocols make the forwarding decisions.

Instructions: Accept the default to allow the policy to overwrite the multicast protocols. Specify 1 to allow the protocols to overwrite the policy filter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.12.1.7

Parameter: Precedence

Path: Configuration Manager > Protocols > IP > Policy Filters > MTM

Default: 0

Options: A metric value

Function: Specifies a metric value to compare this policy with other policies that a route may match. A policy with a higher metric takes precedence over a policy with a lower metric. In case of a tie, the protocol uses an internal index value assigned to the policy by IP software. The position of the policy in the list indicates the index value from lowest to highest.

Instructions: Use this parameter to assign precedence to policies that match the same route.

MIB Object ID: MOSPF: 1.3.6.1.4.1.18.3.5.3.2.6.12.1.8

Parameter:	**Sources**
Path:	Configuration Manager > Protocols > IP > Policy Filters > MTM
Default:	An empty list
Options:	Leave empty or specify one or more sources.
Function:	Identifies which sources will match this rule.
Instructions:	If you want this filter to match any source, do not specify any value for this parameter. To specify an exact source address or range of source addresses, enter one or more octet groupings in the following form: First octet: exact (1) or range (2) Next 4 octets: source address Next 4 octets: source mask An entry with an exact tag matches only the specific source (number and mask). An entry with a range tag matches any prefix that falls in the range indicated by the source and mask.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.6.12.1.10

Parameter:	**In Circuits**
Path:	Configuration Manager > Protocols > IP > Policy Filters > MTM
Default:	An empty list
Options:	Leave empty or specify one or more 2-octet circuit numbers.
Function:	Lists inbound circuits.
Instructions:	If you do not want this circuit to accept any inbound packets, leave the value for this parameter empty. If you want this circuit to accept inbound packets, enter the circuit number or numbers, in 2-octet strings.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.6.12.1.11

Parameter: Out Circuits

Path: Configuration Manager > Protocols > IP > Policy Filters > MTM
Default: An empty list
Options: Leave empty or specify one or more outbound circuit number and time-to-live (TTL) threshold octet combinations.
Function: Lists outbound circuits.
Instructions: If you do not want this circuit to forward any packets affected by this filter, leave the value for this parameter empty.

To define a circuit number and TTL threshold from which you want to forward packets, enter the octets as follows:

First 2 octets: circuit number

Next 2 octets: TTL threshold

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.6.12.1.12

IGMP Boundary Group Parameters

Use the following descriptions to set IGMP boundary group parameters.

Parameter: Enable

Path: Configuration Manager > Protocols > IP > Multicast > IGMP > Boundaries
Default: Enabled
Options: Enabled | Disabled
Function: Specifies whether this record is enabled or disabled.
Instructions: To disable the boundary group record, enter Disabled.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.5.1.2

Parameter: Group Address

Path: Configuration Manager > Protocols > IP > Multicast > IGMP > Boundaries
Default: None
Options: A valid group address.
Function: Specifies the address of a multicast host group.
Instructions: Enter a group address to define this IGMP boundary record.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.5.1.3

Parameter: Prefix Length

Path:	Configuration Manager > Protocols > IP > Multicast > IGMP > Boundaries
Default:	None
Options:	A valid prefix for the group address.
Function:	Specifies a prefix for the multicast host group address.
Instructions:	Enter an address prefix to define this IGMP boundary record.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.13.5.1.

Parameter: Circuit List

Path:	Configuration Manager > Protocols > IP > Multicast > IGMP > Boundaries
Default:	None
Options:	A list of one or more circuit addresses.
Function:	Specifies a list of circuit addresses for this boundary definition.
Instructions:	Specify each circuit with a 2-octet address.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.13.5.1.

Parameter: Tunnel List

Path:	Configuration Manager > Protocols > IP > Multicast > IGMP > Boundaries
Default:	None
Options:	A list of one or more multicast tunnels
Function:	Specifies a list of tunnels for this boundary address.
Instructions:	Specify each tunnel with an eight-octet address, four octets for the local IP address (the local end of the tunnel) and four octets for the remote IP address (the remote end of the tunnel).
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.13.5.1.

Configuring IP Services

The following section is an amendment to *Configuring IP Services.*

Customizing the IP Routing Table Structure

Structurally, the IP routing table consists of *indexes* and *entries.* Each index contains a pointer to a sublist of entries. By default, the IP routing table contains 0 indexes.

A routing table in which all indexes point to the same number of entries is considered to be in perfect *balance*. For example, a routing table that contains 100 indexes pointing to 1,000 entries is in perfect balance if each index points to 10 entries.

In reality, an IP routing table is allowed to contain indexes that deviate from perfect balance by a number of entries specified as the *deviation-of-nodes* value. By default the deviation-of-nodes value is 0.

To use the BCC to specify the number of indexes in the IP routing table and to specify a deviation-of-nodes value, enter the following commands:

rtbl-indexes *number*
rtbl-deviation-of-nodes *deviation*

number is the number of indexes in the IP routing table.

deviation is the number of entries by which an index is allowed to deviate from perfect balance.

For example, the following command sequence configures an IP routing table with 1,000 indexes and a deviation value of 10:

```
ip# rtbl-indexes 1000
ip# rtbl-deviation-of-nodes 10
```

Caution: Bay Networks recommends that you use the default values for the IP routing table parameters. If you want to specify different values, consult the Bay Networks Technical Solutions Center.

Configuring IPv6 Services

The following section is an amendment to *Configuring IPv6 Services*.

RIPv6 Announce Policy Parameters

Parameter:	**Announce Prefixes**
Path:	Configuration Manager > Protocols > IPv6 > RIPv6 > Policies > Announce
Default:	An empty list
Options:	See below.
Function:	Specifies a prefix identification list. This list identifies which prefixes will match this rule. If non-null, the octet string contains one or more 3-tuples of the following form: First item: prefix in standard IPv6 notation Second item: prefix length, between 0 and 128 Third item: keyword 'exact' or 'range' Example: 3ffe:1300:1::0/48/range is match any IPv6 prefix of any length in the range 3ffe:1300:1::0 through 3ffe:1300:1:ffff:ffff:ffff:ffff:ffff.
Instructions:	An entry with an “exact” tag means to match only the specific network advertisement (prefix and length). An entry with a “range” tag means to match any prefix that falls in the range indicated by the prefix and length. If multiple prefixes are listed, a match against any prefix means this portion of the policy matches. An “exact” encoding of ::0/0 means match the default route. A “range” encoding of ::0/0 means match any route. An empty list also means match any route.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.6.2.1.5

Parameter: Announce Interface

Path: Configuration Manager > Protocols > IPv6 > RIPv6 > Policies > Announce

Default: Null

Options: See below.

Function: Supplies a RIP outbound interface list -- a list that contains one or more IPv6 interface index identifiers on this router. If an interface address is included in this list, this policy applies to RIP advertisements received on that interface.

Instructions: If you supply an IPv6 interface index, this policy applies to RIP updates sent on that interface. If the list is empty, this policy applies to RIP updates sent on all IPv6 interfaces.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.6.2.1.12

Parameter: Announce RIP Metric

Path: Configuration Manager > Protocols > IPv6 > RIPv6 > Policies > Announce

Default: Null

Options: 0 to 15

Function: Overrides the router-calculated RIP metric with the supplied value for prefixes that match this policy.

Instructions: This parameter is used only if the action is Announce and this policy is the best match. If zero, the routing table metric calculated for RIP (received metric plus the interface cost) is sent. If a value is specified, that value is set as the RIP metric for prefixes that match this policy.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.6.2.1.13

IPV6 Interface Parameters

Parameter: **Interface Token**

Path: Configuration Manager > Protocols > IPv6 > Edit IPv6 Interfaces

Default: See Instructions.

Options: A portion of an IPv6 address, consisting of 0 to 32 hex characters, entered in four-character groups delimited by a colon.

Function: Supplies an identifier (an interface token) for this interface that is unique on the link to which this interface is attached. The interface token is combined with an address prefix to form an interface address.

Instructions: If you do not configure a token, the interface token is autoconfigured according to the rules of the link type to which this interface is attached. For most media, this involves mapping the link layer (or MAC) address, X. 121 address, or other unique value (for example, a serial number) to a 64-bit value. For example, MAC 00-00-a2-11-22-23 maps to IPv6 token 0200:a2ff:fe11:2233 according to the RFCs specifying methods for transmitting IPv6 datagrams over FDDI, Ethernet, and Token Ring.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.1.2.1.7

Parameter: **Circuit Name**

Path: Configuration Manager > Protocols > IPv6 > Edit IPv6 Interfaces

Default: The name of the circuit on which you have configured the IPv6 interface

Options: A valid circuit name

Function: Identifies the circuit on which the interface runs.

Zero indicates that this is a tunnel end point. In IPv6 tunneling, IPv6 packets are encapsulated and transmitted by another network layer protocol or another instance of the IPv6 protocol. A value greater than 1023 indicates that the interface is the circuitless, or software loopback, interface.

Instructions: Supply a value that identifies this circuit.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.1.2.1.6

Parameter:	**Slot Mask**
Path:	Configuration Manager > Protocols > IPv6 > Edit IPv6 Interfaces
Default:	All slots
Options:	Slot 1 to 14
Function:	Specifies the slots on which a circuitless interface can run.
Instructions:	Select one or more slots as candidates to run this circuitless IPv6 interface. This attribute is considered only if this IPv6 interface has a circuit defined with a value greater than 1023.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.1.1.2.1.15

Configuring PPP Services

The following sections are amendments to *Configuring PPP Services*:

- Summary of PPP Services
- Priority Queueing over PPP Multilink
- WCP over PPP Multilink
- RFC 1661 Compliance for PPP Dial Circuits

Summary of PPP Services

In the PPP Configurable Functions table (Chapter 1), the table entry that reads **Run PPP over dial-up lines** incorrectly shows BCC as a configuration tool for this feature.You cannot use BCC to configure PPP over dial-up lines for 12.10.

Priority Queueing over PPP Multilink

Priority queueing is now available over PPP multilink. Priority queueing enables you to resequence outbound data packets into prioritized delivery queues called priority queues. To use priority queueing over multilink, first set the PPP Mode parameter to multilink and then configure the parameters in the Protocol Priority Interfaces window. If compression is configured, the router prioritizes data before it compresses it. Refer to information about *protocol prioritization* in *Configuring Traffic Filters and Protocol Prioritization* for information about how to configure priority queueing.

WCP over PPP Multilink

For BayRS 12.10, by default the router negotiates the WAN compression protocol (WCP) above the PPP multilink bundle for new circuits only. Negotiating compression above the bundle means that data packets are first compressed and then distributed across the links in the bundle. The distribution of traffic occurs once for the entire bundle and the balance of traffic across the bundle is more accurate. In addition, the router uses less memory for compression.

Routers using BayRS 12.10 with an older configuration file negotiate WCP below the multilink bundle by default. By negotiating compression below the bundle, data packets are first distributed across the links and then compressed. Compression is done individually for every link. You can reconfigure the circuit to negotiate WCP above the bundle by changing the CCP Type parameter to CCP on the routers at both ends of the link.

If you configure a new multilink circuit on a version 12.10 router and the remote router is running a version of software earlier than 12.10, you must change the CCP Type parameter from the default to ILCCP for the local router and set the PPP Mode to multilink.

For information about how to configure data compression and the related PPP compression parameters, refer to *Configuring Data Compression Services*.

RFC 1661 Compliance for PPP Dial Circuits

You can use Site Manager to configure a dial circuit to be compliant with Request for Comment (RFC) 1661:

Site Manager Path	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols.**	The Protocols menu opens.
2. Choose **PPP.**	The PPP menu opens.
3. Choose **Interfaces**.	The PPP Interface List window opens.
4. Click on **Lines**.	The PPP Line List window opens.
5. Set the **RFC1661 Compliance** parameter. Click on **Help** or see the parameter description that follows this table.	
6. Click on **Done**.	You return to the PPP Interface List window.
7. Click on **Done**.	You return to the Configuration Manager window.

Parameter:	**RFC1661 Compliance**
Path:	Configuration Manager > Protocols > PPP > Interfaces > **Lines**
Default:	Disable
Options:	Enable | Disable
Function:	Enables RFC 1661 compliance for a PPP dial circuit.
Instructions:	Select Enable to make the PPP dial circuit RFC 1661 compliant. Otherwise, accept the default.
MIB OID:	1.3.6.1.4.1.18.3.5.9.2.1.1.49

Configuring X.25 Services

The following sections are amendments to *Configuring X.25 Services*:

- Remote Backup IP Interface for IPEX
- Calling Address Insertion

Remote Backup IP Interface for IPEX

You can now configure a backup IP address for IPEX TCP connections. This feature allows the router to establish a TCP connection with a remote IPEX router even if the remote IP interface is down.

Parameter: Remote Backup IP Address

Path: Configuration Manager > Protocols > IPEX > IPEX Mapping Table

Default: 0.0.0.0

Options: Any valid IP address

Function: Allows you to configure a backup IP address for IPEX TCP connections. If you enter an IP address in this parameter, when IPEX attempts to open a TCP connection and detects that the remote IP interface is down, it will use this backup remote IP address and try again to establish the connection. If both the primary and secondary remote IP interfaces are down, IPEX rejects the call. If the value in the parameter is the default, 0.0.0.0, IPEX detects that there is no backup and does not try to establish the connection a second time.

For IPEX to detect that the remote IP interface is down and retry the TCP connection, set the X.25 Keep Alive timer to a value shorter than the X.25 Idle Session timer; otherwise the VC will be cleared before IPEX has time to retry the call.

Instructions: Enter the appropriate X.121 address, and set the Insert Calling DTE Address parameter to Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.15.2.1.23

Calling Address Insertion

Normally the calling address field in incoming call packets identifies a device reporting an alarm. However, some X.25 devices do not provide this address in the call request packets, and rely instead on the public X.25 network to insert the correct calling address (if you have enabled the Insert Calling DTE Address parameter). A new parameter, Translate Calling X.121 Address, allows the router to overwrite the value that the network supplies, and insert in the call request packets it transports the calling address you enter in this parameter.

Parameter:	**Translate Calling X.121 Address**
Path:	Configuration Manager > Protocols > IPEX > IPEX Mapping Table
Default:	None
Options:	Any valid X.121 address
Function:	Allows the router to overwrite the value that the network supplies, and use this address as the calling address. To use this feature, you must also set the Insert Calling DTE Address parameter to Enable.
Instructions:	Enter the appropriate X.121 address, and set the Insert Calling DTE Address parameter to Enable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.15.2.1.24

Event Messages for Routers

Table 2 lists the service and entity names that correspond to the new or amended sections in *Event Messages for Routers.*

Table 2. New and Amended Event Messages

Service	Entity	Section	Page
ATM Half Bridge	AHB	AHB Fault Events AHB Warning Events AHB Info Events	69 73 75
ATM LAN Emulation	ATM_LE	ATM_LE Warning Events ATM_LE Info Events	77 77
Carrier Sense Multiple Access/Collision Detect	CSMACD	CSMACD Info Event	78
RMON Data Collection Module (DCM) Middleware	DCMMW	DCMMW Fault Event DCMMW Warning Events	78 80
Data Path	DP	DP Warning Events DP Info Events DP Trace Event	80 82 84
Frame Relay PVC Pass Through Events	FRPT	FRPT Fault Event FRPT Warning Events FRPT Info Events FRPT Trace Event	84 85 86 89
Frame Relay Switched Virtual Circuits	FR_SVC	FR_SVC Fault Event FR_SVC Warning Event FR_SVC Info Events	90 90 91
Frame Relay Switched Virtual Circuits API	FR_SVC_API	FR_SVC_API Warning Events FR_SVC_API Info Events FR_SVC_API Trace Events	92 94 95
Hypertext Transfer Protocol	HTTP	HTTP Fault Event HTTP Warning Events HTTP Info Events HTTP Trace Events	96 96 97 98
Intelligent Serial Daughter Board	ISDB	ISDB Fault Events ISDB Warning Events ISDB Info Events	102 103 105

(continued)

Table 2. New and Amended Event Messages *(continued)*

Service	Entity	Section	Page
Layer 2 Tunneling Protocol	L2TP	L2TP Fault Event L2TP Warning Events L2TP Info Events L2TP Trace Events	108 108 111 114
Learning Bridge	LB	LB Warning Event	116
Dynamic Loader	LOADER	LOADER Info Events	116
Open Shortest Path First	OSPF	OSPF Fault Events OSPF Warning Events OSPF Info Event	117 118 119
Point-to-Point	PPP	PPP Warning Events	119
FireWall	RFWALL	RFWALL Warning Events RFWALL Info Events RFWALL Trace Event	120 121 121
RMONSTAT	RMONSTAT	RMONSTAT Info Event	122
STAC LZS	STAC	STAC Fault Event STAC Warning Events STAC Info Events STAC Trace Event	122 123 124 125
TELNET server	TELNET	TELNET Fault Event TELNET Warning Event TELNET info Events TELNET Trace Events	125 126 126 129
Virtual circuit service for DLSw/APPN Boundary functionality	VCCT	VCCT Fault Event	130
X.25 PAD	X.25 PAD	X.25 PAD Fault Event X.25 PAD Warning Event X.25 PAD Info Event X.25 PAD Trace Event	130 131 131 132

In addition, the following change applies to the definition of “Trace” events described in the *Event Messages for Routers* guide:

Former (incorrect) definition -- Trace indicates information about each packet that traversed the network. Bay Networks recommends viewing this type of trap message only when diagnosing network problems.

Corrected definition -- A series of related, time-stamped, Trace messages describe the progress of a specific process running in the device software. A progression of Trace messages may indicate either a normal or abnormal sequence in the operation of any internal process. An analysis of Trace messages for a specific entity (for example, a protocol) collectively depict the general health of that entity. For this reason, and because of the amount of information that Trace messages collectively record, Bay Networks recommends viewing them only when necessary for the purpose of troubleshooting device operation.

AHB Fault Events

ATM Half Bridge, also known as the AHB entity, issues the following fault event messages. The entity code assigned to AHB events is 149.

Entity Code/Event Code **149/6**

Decimal Identifier **16815366**

Severity: Fault

Message: Unable to initialize BTM

Meaning: AHB was unable to initialize the bridge table manager (BTM). This condition might be caused by insufficient memory resources. Check system memory usage.

Action: Contact the Bay Networks Technical Solutions Center.

Entity Code/Event Code **149/7**

Decimal Identifier **16815367**

Severity: Fault

Message: Bad opcode <*opcode_number*> in BTM update mesg, message ignored.

Meaning: Internal error occurred.

Action: Contact the Bay Networks Technical Solutions Center.

Entity Code/Event Code **149/8**

Decimal Identifier **16815368**

Severity: Fault

Message: Duplicate host sequence number <*sequence_number*> detected, terminating

Meaning: An attempt was made to add a new bridge table entry and the unique serial number assigned was already in use by another bridge table entry.

Action: Contact the Bay Networks Technical Solutions Center.

Entity Code/Event Code **149/9**

Decimal Identifier **16815369**

Severity: Fault

Message: Unable to add network to local bridge table.

Meaning: Unable to add a new IP network in the bridge table. This may be caused by insufficient memory resources.

Action: Check system memory usage.

Entity Code/Event Code **149/10**

Decimal Identifier **16815370**

Severity: Fault

Message: Unable to add remote network mask <*mask_address*> on slots <*slot_numbers*>

Meaning: Unable to add a new IP network in the bridge table. This may be caused by insufficient memory resources.

Action: Check system memory usage.

Entity Code/Event Code **149/11**

Decimal Identifier **16815371**

Severity: Fault

Severity: Unable to delete network <*network_number*> mask <*mask_number*>, slot <*slot_number*>, ignored

Meaning: Unable to delete a new IP network in the bridge table. This may condition may be caused by lack of sufficient memory resources.

Action: Check system memory usage.

Entity Code/Event Code **149/12**

Decimal Identifier **16815372**

Severity: Fault

Message: No circuit to available when inserting route for net <*network_number*>, mask <*mask_address*>, circuit <*circuit_number*>

Meaning: No available AHB circuit could be found when adding a new route entry in the IP routing table.

Action: Check to make sure that at least one AHB circuit is in the "up" state.

Entity Code/Event Code **149/13**

Decimal Identifier **16815373**

Severity: Fault

Message: Insert route failed for net <*network_number*>, mask <*mask_address*>, circuit <*circuit_number*>

Meaning: Unable to insert an AHB-type route in the IP routing table.

Action: Check to be sure IP is loaded and operational on the local slot, and that the circuit identified in this event is in the "up" state.

Entity Code/Event Code **149/14**

Decimal Identifier **16815374**

Severity: Fault

Message: Delete route failed for net <*network_number*>, mask <*mask_address*>, circuit <*circuit_number*>

Meaning: Unable to remove an AHB-type route from the IP routing table.

Action: Check to be sure IP is loaded and operational on the local slot.

Entity Code/Event Code **149/15**

Decimal Identifier **16815375**

Severity: Fault

Message: Unable to get buffer for map message <*message_number*> data <*data_number*>.

Meaning: No buffers available for control data.

Action: Restart AHB.

Entity Code/Event Code **149/16**

Decimal Identifier **16815376**

Severity: Fault

Message: Unable to add new VC <*virtual_circuit_number*> to cct <*circuit_number*>

Meaning: Unable to add a new ATM PVC as directed by AHB init file.

Action: Verify that ATM is configured properly, and that the maximum number of VCs on this circuit has not been exceeded.

Entity Code/Event Code **149/17**
Decimal Identifier **16815377**
Severity: Fault
Message: Unable to get circuit <*circuit_number*> info
Meaning: Unable to obtain information about the circuit identified in the event.
Action: Contact the Bay Networks Technical Solutions Center.

Entity Code/Event Code **149/18**
Decimal Identifier **16815378**
Severity: Fault
Message: File Read Error Code <*error_code_number*>
Meaning: Error occurred during reading of AHB init file (or alternate init file).
Action: Verify that AHB can read the existing init data file.

Entity Code/Event Code **149/19**
Decimal Identifier **16815379**
Severity: Fault
Message: Child gate died, type=<*type_number*>, subsystem restarting
Meaning: AHB terminated abnormally.
Action: None.

Entity Code/Event Code **149/20**
Decimal Identifier **16815380**
Severity: Fault
Message: Bad message ID <*id_number*> received by master gate, ignored.
Meaning: Unrecognized control message received by AHB.
Action: If this problem persists, contact the Bay Networks Technical Solutions Center.

Entity Code/Event Code **149/21**
Decimal Identifier **16815381**
Severity: Fault
Message: Failed send to master gate, killing myself.
Meaning: Internal error occurred.
Action: Contact the Bay Networks Technical Solutions Center.

Entity Code/Event Code **149/22**

Decimal Identifier **16815382**

Severity: Fault

Message: Unable to add AHB cct <*circuit_number*>.

Meaning: Internal error occurred.

Action: Contact the Bay Networks Technical Solutions Center.

Entity Code/Event Code **149/23**

Decimal Identifier **16815383**

Severity: Fault

Message: Proxy reregistration error.

Meaning: Internal error occurred.

Action: Contact the Bay Networks Technical Solutions Center.

AHB Warning Events

ATM HalfBridge, also known as the AHB entity, issues the following warning event messages. The entity code assigned to AHB events is 149.

Entity Code/Event Code **149/24**

Decimal Identifier **16815384**

Severity: Warning

Message: Circuit <*circuit_number*> not found while adding ATM PVCs.

Meaning: Circuit identified in bridge entry could not be found when attempting to create a new PVC (as directed by the host entry in the init file).

Action: Verify that you have configured the identified circuit.

Entity Code/Event Code **149/25**

Decimal Identifier **16815485**

Severity: Warning

Message: AHB interface not found for circuit <*circuit_number*>.

Meaning: The AHB interface identified by circuit number could not be located when an attempt was made to add a new bridge table entry.

Action: Contact the Bay Networks Technical Solutions Center.

Entity Code/Event Code **149/26**

Decimal Identifier **16815486**

Severity: Warning

Message: Unable to set inbound filtering, no ATM control for circuit <*circuit_number*>.

Meaning: Internal error.

Action: Contact the Bay Networks Technical Solutions Center.

Entity Code/Event Code **149/27**

Decimal Identifier **16815487**

Severity: Warning

Message: Unsupported encaps type on circuit <*circuit_number*>.

Meaning: AHB was configured on an ATM service record that uses an encapsulation type other than RFC 1483 SNAP/LLC. This interface will not be used.

Action: Check configuration of ATM service record on which AHB is configured.

Entity Code/Event Code **149/28**

Decimal Identifier **16815488**

Severity: Warning

Message: Reference VC <*VC_number*> on circuit <*circuit_number*> not found.

Meaning: The reference PVC to be used as a template when creating a new ATM PVC could not be located on the router. The VPI/VCI for this reference PVC is identified within a host entry in the AHB init file.

Action: Check the ATM PVC list on this service record to verify that you have configured the VPI/VCI, and reload AHB.

Entity Code/Event Code **149/29**

Decimal Identifier **16815489**

Severity: Warning

Message: Error reading SLOT data, line <*line_number*>.

Meaning: Missing or invalid slot label in AHB init file.

Action: Check syntax for the identified line number.

Entity Code/Event Code **149/30**

Decimal Identifier **16815490**

Severity: Warning

Message: Error reading data, line <*line_number*>.

Meaning: Invalid host entry in AHB init file.

Action: Check the syntax for the identified line number.

Entity Code/Event Code **149/31**

Decimal Identifier **16815491**

Severity: Warning

Message: No AHB base record configured.

Meaning: AHB Base MIB object could not be located.

Action: Verify that the configuration file exists prior to rebooting.

Entity Code/Event Code **149/32**

Decimal Identifier **16815492**

Severity: Warning

Message: Failed to open file <*filename*>, using alternate

Meaning: The init file identified in the AHB base record could not be read.

Action: Verify that this file exists on the router's flash file system.

Entity Code/Event Code **149/33**

Decimal Identifier **16815493**

Severity: Warning

Message: Failed to open file <*filename*>, giving up.

Meaning: The alternate init file identified in the AHB base record could not be read.

Action: Verify that this file exists on the router's flash file system.

AHB Info Events

ATM Half Bridge, also known as the AHB entity, issues the following info event messages. The entity code assigned to AHB events is 149.

Entity Code/Event Code **149/34**

Decimal Identifier **16815494**

Severity: Info

Message: AHB interface <*interface_number*> is up.

Meaning: AHB interface is operational and ready to forward packets in either direction.

Entity Code/Event Code **149/35**

Decimal Identifier **16815495**

Severity: Info

Message: AHB interface <*interface_number*> is down.

Meaning: AHB interface is not operational.

Action: Check ATM line status and ATM circuit status.

Entity Code/Event Code **149/36**

Decimal Identifier **16815496**

Severity: Info

Message: Reading from data file <*filename*>

Meaning: AHB is now reading the initialization file. This condition occurs after you first load the subsystem or after you perform a reset operation.

Entity Code/Event Code **149/37**

Decimal Identifier **16815497**

Severity: Info

Message: Finished reading data file.

Meaning: AHB has finished reading the initialization file. The bridge table is now populated with all bridge entries identified in the init file.

Entity Code/Event Code **149/38**

Decimal Identifier **16815498**

Severity: Info

Message: AHB initialization complete

Meaning: AHB has initialized and is now operational on the local slot.

Entity Code/Event Code **149/39**

Decimal Identifier **16815499**

Severity: Info

Message: Read_data: waiting 10 seconds for IP.

Meaning: AHB is waiting for IP to become operational prior to reading the init file.

Action: If this event persists, verify that IP is loaded and operational on the current slot

ATM_LE Warning Events

The ATM LAN Emulation service, also known as the ATM_LE entity, supports the following warning event messages. The entity code assigned to ATM_LE events is 100.

Entity Code/Event Code **100/52**

Decimal Identifier **16802868**

Severity: Warning

Message: Line <*line_no.*> : Circuit <*circuit_no.*> : Instance <*instance*> LES is unreachable.

Meaning: The indicated LES is not responding.

Entity Code/Event Code **100/54**

Decimal Identifier **16802870**

Severity: Warning

Message: Line <*line_no.*> : Circuit <*circuit_no.*> : ATM LEC now trying next le server.

Meaning: The ATM LAN emulation client is trying the next configured LAN emulation server (LES).

ATM_LE Info Events

The ATM LAN Emulation service, also known as the ATM_LE entity, supports the following info event messages. The entity code assigned to ATM_LE events is 100.

Entity Code/Event Code **100/50**

Decimal Identifier **16802866**

Severity: Info

Message: Line <*line_no.*> : Circuit <*circuit_no.*> : Instance <*instance*> LES is deleted.

Meaning: The indicated LES has been deleted.

Entity Code/Event Code **100/51**

Decimal Identifier **16802867**

Severity: Info

Message: Line <*line_no.*> : Circuit <*circuit_no.*> : Instance <*instance*> LES is disabled.

Meaning: The indicated LES is disabled.

CSMACD Info Event

The Carrier Sense Multiple Access/Collision Detect service, also known as the CSMACD entity, supports the following new info message. The entity code assigned to CSMACD events is 9.

Entity Code/Event Code **9/44**

Decimal Identifier **16779564**

Severity: Info

Message: Connector XCVR<*connector_no.*>: XCHIP and THUNDERSwitchInterface Initialization Complete

Meaning: The XCHIP and THUNDERSwitch have been initialized on the CSMA/CD connector identified by XCVR<*connector_no.*>.

DCMMW Fault Event

The RMON data collection module (DCM) middleware, also known as the DCMMW entity, supports the following new fault event message. The entity code assigned to DCMMW events is 96.

Entity Code/Event Code **96/88**

Decimal Identifier **16815691**

Severity: Fault

Message: DCMMW_NO_CSMACD

Meaning: You must configure the Ethernet interface before you attempt to configure Ethernet DCM on the router.

Action: Configure an Ethernet interface before configuring the Ethernet DCM on the router.

DCMMW Warning Events

The RMON data collection module (DCM) middleware, also known as the DCMMW entity, supports the following new warning event messages. The entity code assigned to DCMMW events is 96.

Entity Code/Event Code **96/89**

Decimal Identifier **16815691**

Severity: Warning

Message: DCMMW_DCM_BAD_VERSION

Meaning: An older version of the Ethernet DCM image is running on the router.

Action: Upgrade the Ethernet DCM image to version 2.0.0.1 to run RMON or RMON2 on the AN®/ANH™ and ARN™ routers.

Entity Code/Event Code **96/90**

Decimal Identifier **16815692**

Severity: Warning

Message: DCMMW_DCM_LOWMEM_RMON2

Meaning: There is insufficient memory available on the Ethernet DCM to collect RMON2 statistics. The Ethernet DCM will collect only RMON statistics.

Action: Increase the Ethernet DCM's memory to 8 MB to collect RMON2 statistics.

DP Warning Events

The Data Path service, also known as the DP entity, issues the following modified and new warning messages. The entity code assigned to DP events is 6.

Entity Code/Event Code **6/69**

Decimal Identifier **16778821**

Severity: Warning

Message: Priority Queuing Length Based Filter disabled, cannot use the LBP filter for IP Circuit *<circuit_no.>*.

Meaning: A length-based filter was configured for IP. This is not allowed; therefore, the filter was disabled.

Action: Remove this IP filter and specify IP-specific prioritizations.

Entity Code/Event Code **6/83**

Decimal Identifier **16778835**

Severity: Warning

Message: Line <*slot_no.*>:<*connector_no.*> MTU <*MTU_value*>, not same circuit MTU <*MTU_value*>, ignoring line.

Meaning: You tried to group a line with a circuit group that had a different maximum transmission unit (MTU) value.

Action: Change the MTU value of the line you are trying to add to match the MTU of the circuit group.

Entity Code/Event Code **6/93**

Decimal Identifier **16778845**

Severity: Warning

Message: <*circuit_no.*>: Multiprotocol encapsulation is not configured for Bridging.

Meaning: You must configure multiprotocol encapsulation (MPE) for this circuit.

Action: Configure MPE for the ATM interface or circuit.

Entity Code/Event Code **6/100**

Decimal Identifier **16778852**

Severity: Warning

Message: The active IP accounting table is now <*percent*> percent full.

Meaning: This message occurs when the active IP Accounting table reaches a specified percent of its maximum number of unique entries. The warning prevents loss of information by enabling you to copy the Active table to a Checkpoint table and reset the Active table before it overflows.

Note: Both the maximum number of entries in the Active IP Accounting table and the percent of maximum entries to initiate this log message are parameter values that you can configure. For information, refer to *Configuring IP Services* or to the Site Manager Help screen for these parameters.

Action: Copy the active IP Accounting table to the checkpoint IP Accounting table by using SNMP commands to get the value of wfCkAcctFlag and reset it to the same value. This action flushes the Active table, allowing room for new entries.

DP Info Events

The Data Path service, also known as the DP entity, issues the following modified and new info event messages. The entity code assigned to DP events is 6.

Entity Code/Event Code **6/81**

Decimal Identifier **16778833**

Severity: Info

Message: Line <*slot_no.*>:<*connector_no.*> added to group of <*no._lines*> lines for cct <*circuit_no.*>.

Meaning: The specified connector was added to the specified number of lines that make up the specified circuit group.

Entity Code/Event Code **6/85**

Decimal Identifier **16778837**

Severity: Info

Message: Last line in circuit died, circuit <*circuit_no.*> going down.

Meaning: The last active line in a multiline circuit group has gone down, causing the circuit to go to the down state.

Entity Code/Event Code **6/86**

Decimal Identifier **16778838**

Severity: Info

Message: Line deleted from circuit <*circuit_no.*>, <*no._lines*> active lines left.

Meaning: A line in a multiline circuit group has gone down, leaving only the specified number of active lines.

Entity Code/Event Code **6/102**

Decimal Identifier **16778854**

Severity: Info

Message: Firewall syn VM installed.

Meaning: Firewall is active on this synchronous interface.

Entity Code/Event Code **6/103**
Decimal Identifier **16778855**
Severity: Info
Message: Firewall VM installed.
Meaning: Firewall is active on this Ethernet interface.

Entity Code/Event Code **6/104**
Decimal Identifier **16778856**
Severity: Info
Message: Firewall 1294sync VM installed.
Meaning: Firewall is active on this synchronous interface.

Entity Code/Event Code **6/105**
Decimal Identifier **16778857**
Severity: Info
Message: Firewall FDDI VM installed.
Meaning: Firewall is active on this FDDI interface

Entity Code/Event Code **6/106**
Decimal Identifier **167788858**
Severity: Info
Message: Firewall Enet VM installed.
Meaning: Firewall is active on this Ethernet interface.

Entity Code/Event Code **6/107**
Decimal Identifier **167788859**
Severity: Info
Message: Firewall PPP VM installed.
Meaning: Firewall is active on this PPP interface.

DP Trace Event

The Data Path service, also known as the DP entity, issues the following trace event message. The entity code assigned to DP events is 6.

Entity Code/Event Code **6/91**

Decimal Identifier **16778843**

Severity: Trace

Message: cct <*circuit_no.*>: Outgoing pkt dropped; no header space.

Meaning: The system received a packet from Ethernet or FDDI that was to be bridged over Frame Relay or ATM. When Frame Relay or ATM tried to add the necessary header information to the packet, there was not enough space for the header. Therefore, the system dropped the packet.

Action: No action required.

FRPT Fault Event

The Frame Relay PVC Pass Through service, also known as the FRPT entity, issues the following fault event message. The entity code assigned to FRPT events is 143.

Entity Code/Event Code **143/1**

Decimal Identifier **16813825**

Severity: Fault

Message: System error, FRPT gate attempting restart.

Meaning: The router experienced a fatal error and is restarting automatically. The router will attempt to restart up to five times.

Action: Verify that the configuration is correct. Call the Bay Networks Technical Solutions Center if the router fails to restart.

FRPT Warning Events

The Frame Relay PVC Pass Through service, also known as the FRPT entity, issues the following warning event messages. The entity code assigned to FRPT events is 143.

Entity Code/Event Code **143/2**

Decimal Identifier **16813826**

Severity: Warning

Message: Config error: New interface <*circuit number, DLCI number*> ignored, conflicts with <*circuit number, DLCI number* >.

Meaning: A configuration error exists: This newly created mapping interface uses a circuit that already exists; each PVC configured for pass through must have a dedicated circuit. The router will not recognize the interface.

Action: Reconfigure pass through so that each circuit participates in only one pass through mapping.

Entity Code/Event Code **143/3**

Decimal Identifier **16813827**

Severity: Warning

Message: Config error: New mapping <*circuit number, DLCI number to circuit number DLCI number*> ignored, interface(s) not found.

Meaning: A configuration error exists: The specified pass through entry includes an interface that does not exist.

Action: Reconfigure pass through to include only valid circuit numbers and DLCIs.

Entity Code/Event Code **143/4**

Decimal Identifier **16813828**

Severity: Warning

Message: Config error: New mapping <*circuit number, DLCI number to circuit number DLCI number*> ignored, interface(s) in use.

Meaning: A configuration error exists. The new mapping entry specified includes at least one interface that already particpates in a pass through mapping.

Action: Reconfigure pass through to include each interface in only one mapping.

Entity Code/Event Code **143/5**

Decimal Identifier **16813829**

Severity: Warning

Message: Interface <*circuit number, DLCI number*> detected unexpected death of partner <*circuit number, DLCI number*> (<text>).

Meaning: The specified interface has detected that the interface to which it maps has failed.

Action: None required.

Entity Code/Event Code **143/6**

Decimal Identifier **16813830**

Severity: Warning

Message: <*text*>

Meaning: This is a generic warning message.

FRPT Info Events

The Frame Relay PVC Pass Through service, also known as the FRPT entity, issues the following info event messages. The entity code assigned to FRPT events is 143.

Entity Code/Event Code **143/7**

Decimal Identifier **16813831**

Severity: Info

Message: Service initializing.

Meaning: Pass through service is starting up.

Entity Code/Event Code **143/8**

Decimal Identifier **16813832**

Severity: Info

Message: Service down.

Meaning: Pass through service is not working.

Entity Code/Event Code **143/9**

Decimal Identifier **16813833**

Severity: Info

Message: Interface initializing (<*circuit number, DLCI number* >).

Meaning: The specified pass through interface is starting up.

Entity Code/Event Code **143/10**

Decimal Identifier **16813834**

Severity: Info

Message: Interface down (<*circuit number, DLCI number* >).

Meaning: The specified pass through interface is not working.

Entity Code/Event Code **143/11**

Decimal Identifier **16813835**

Severity: Info

Message: Interface added (<*circuit number, DLCI number* >).

Meaning: The specified pass through interface has been added to the network.

Entity Code/Event Code **143/12**

Decimal Identifier **16813836**

Severity: Info

Message: Interface deleted (<*circuit number, DLCI number* >).

Meaning: The specified pass through interface has been deleted from the network.

Entity Code/Event Code **143/13**

Decimal Identifier **16813837**

Severity: Info

Message: Interface Enabled (<*circuit number, DLCI number* >).

Meaning: The specified pass through interface is enabled.

Entity Code/Event Code **143/14**

Decimal Identifier **16813838**

Severity: Info

Message: Interface Disabled (<*circuit number, DLCI number* >).

Meaning: The specified pass through interface is disabled.

Entity Code/Event Code **143/15**

Decimal Identifier **16813839**

Severity: Info

Message: Interface <*circuit number, DLCI number* > unable to raise partner <*circuit number, DLCI number* >.

Meaning: The specified pass through interface is unable to reach the interface to which it maps.

Entity Code/Event Code **143/16**

Decimal Identifier **16813840**

Severity: Info

Message: Mapping added (<*circuit number, DLCI number to circuit number DLCI number*>).

Meaning: The specified mapping has been added to the network.

Entity Code/Event Code **143/17**

Decimal Identifier **16813841**

Severity: Info

Message: Mapping deleted (<*circuit number, DLCI number to circuit number DLCI number*>).

Meaning: The specified mapping has been deleted from the network.

Entity Code/Event Code **143/18**

Decimal Identifier **16813842**

Severity: Info

Message: Mapping Enabled (<*circuit number, DLCI number to circuit number DLCI number*>).

Meaning: The specified mapping is enabled.

Entity Code/Event Code **143/19**

Decimal Identifier **16813843**

Severity: Info

Message: Mapping Disabled (<*circuit number, DLCI number to circuit number DLCI number*>).

Meaning: The specified mapping is disabled.

Entity Code/Event Code **143/20**

Decimal Identifier **16813844**

Severity: Info

Message: Mapping became Active (<*circuit number, DLCI number to circuit number DLCI number*>).

Meaning: The specified mapping is active.

Entity Code/Event Code **143/21**

Decimal Identifier **16813845**

Severity: Info

Message: Mapping became Inactive (<*circuit number, DLCI number to circuit number DLCI number*>).

Meaning: The specified mapping is inactive.

FRPT Trace Event

The Frame Relay PVC Pass Through service, also known as the FRPT entity, issues the following trace event message. The entity code assigned to FRPT events is 143.

Entity Code/Event Code **143/22**

Decimal Identifier **16813846**

Severity: Trace

Message: <*text*>

Meaning: This is a generic message.

FR_SVC Fault Event

The Frame Relay Switched Virtual Circuits service, also known as the FR_SVC entity, issues the following fault event message. The entity code assigned to FR_SVC events is 136.

Entity Code/Event Code	**136/1**
Decimal Identifier	**16812033**
Severity:	Fault
Message:	FR SVC System Error
Meaning:	The frame relay subsystem experienced a fatal error and is restarting automatically.
Action:	Verify that the configuration is correct. Call the Bay Networks Technical Solutions Center if the router fails to restart.

FR_SVC Warning Event

The Frame Relay Switched Virtual Circuits service, also known as the FR_SVC entity, issues the following warning event message. The entity code assigned to FR_SVC events is 136.

Entity Code/Event Code	**136/2**
Decimal Identifier	**16812034**
Severity:	Warning
Message:	Client registration error cct <*circuit_name*> of type <*type description*>
Meaning:	The specified client registration error has occurred on the specified circuit.
Action:	Contact the Technical Solutions Center.

FR_SVC Info Events

The Frame Relay Switched Virtual Circuits service, also known as the FR_SVC entity, issues the following info event messages. The entity code assigned to FR_SVC events is 136.

Entity Code/Event Code **136/3**
Decimal Identifier **16812035**
Severity: Info
Message: Service initializing
Meaning: Frame relay SVC service is initializing.

Entity Code/Event Code **136/4**
Decimal Identifier **16812036**
Severity: Info
Message: Master gate down.
Meaning: The frame relay master gate is down.

Entity Code/Event Code **136/5**
Decimal Identifier **16812037**
Severity: Info
Message: Frame relay SVC MIB initializing.
Meaning: The frame relay SVC MIB is initializing.

Entity Code/Event Code **136/6**
Decimal Identifier **16812038**
Severity: Info
Message: Frame relay SVC sig ctrl initializing
Meaning: The frame relay SVC signaling control function is initializing.

Entity Code/Event Code **136/7**
Decimal Identifier **16812039**
Severity: Info
Message: Frame relay SVC sig ctrl rcvd LAPF link up.
Meaning: Frame relay SVC signaling control has received a message that the LAPF link is up.

Entity Code/Event Code **136/8**

Decimal Identifier **16812040**

Severity: Info

Message: Frame relay SVC sig ctrl rcvd LAPF link down.

Meaning: Frame relay SVC signaling control has received a message indicating that the LAPF link is down.

FR_SVC_API Warning Events

The Frame Relay SVC API service, also known as the FR_SVC_API entity, issues the following warning event messages. The entity code assigned to FR_SVC_API events is 146.

Entity Code/Event Code **146/1**

Decimal Identifier **16814593**

Severity: Warning

Message: Message sent to API Gate failed.

Meaning: An internal message the router sent failed to reach the API gate.

Action: Internal error. Contact the Technical Solutions Center.

Entity Code/Event Code **146/2**

Decimal Identifier **16814594**

Severity: Warning

Message: Frame relay master gate died.

Meaning: The frame relay master gate failed. Internal error.

Action: Contact the Technical Solutions Center.

Entity Code/Event Code **146/5**

Decimal Identifier **16814597**

Severity: Warning

Message: Unexpected error signaling ASR CCT Gate.

Meaning: An error occurred when ASR tried to register with the frame relay signaling function.

Action: Contact the Technical Solutions Center.

Entity Code/Event Code **146/7**

Decimal Identifier **16814599**

Severity: Warning

Message: Unexpected error signalling Setup Gate.

Meaning: An error occurred in trying to set up an SVC.

Action: Contact the Technical Solutions Center.

Entity Code/Event Code **146/8**

Decimal Identifier **168145100**

Severity: Warning

Message: Q933 did not find service record for cct <*circuit_name*>.

Meaning: The ASR software could not locate a service record for the specified circuit.

Action: Check that the service record is properly configured.

Entity Code/Event Code **146/10**

Decimal Identifier **168145102**

Severity: Warning

Message: Error in ASR Request id <*ID_number*>.

Meaning: An error occurred in the ASR Request ID routine for the specified ID number.

Action: Check that ASR is properly configured.

Entity Code/Event Code **146/16**

Decimal Identifier **168145108**

Severity: Warning

Message: No signaling gate found for circuit <*circuit_name*>.

Meaning: The ASR software could not locate the signaling gate for the specified circuit, and could not set up an SVC.

Action: Check that SVC signaling is enabled on this circuit.

FR_SVC_API Info Events

The Frame Relay SVC API service, also known as the FR_SVC_API entity, issues the following info event messages. The entity code assigned to FR_SVC_API events is 146.

Entity Code/Event Code **146/6**
Decimal Identifier **16814598**
Severity: Info
Message: Connect confirm received from FR subsystem.
Meaning: A connect confirmation message has been received from the frame relay subsystem.

Entity Code/Event Code **146/9**
Decimal Identifier **168145101**
Severity: Info
Message: Success message sent to Setup Gate.
Meaning: The connection has completed successfully.

Entity Code/Event Code **146/11**
Decimal Identifier **168145103**
Severity: Info
Message: Q933 registration success received on cct <*circuit _name*>.
Meaning: Q933 has completed registration successfully on the specified circuit.

Entity Code/Event Code **146/12**
Decimal Identifier **168145104**
Severity: Info
Message: Q933 ack'd request <*request ID*>.
Meaning: Q933 has acknowledged the specified request.

Entity Code/Event Code **146/13**
Decimal Identifier **105**
Severity: Info
Message: CCT Gate on circuit <*circuit _name*> registered.
Meaning: The circuit gate on the specified circuit has registered.

Entity Code/Event Code **146/14**

Decimal Identifier **168145106**

Severity: Info

Message: Request for a new SVC received.

Meaning: The frame relay subsystem has received a request for a new SVC.

Entity Code/Event Code **146/15**

Decimal Identifier **107**

Severity: Info

Message: Request sent to signaling gate on circuit <*circuit _name*>.

Meaning: The frame relay subsystem has sent a request to the signaling gate on the specified circuit.

FR_SVC_API Trace Events

The Frame Relay SVC API service, also known as the FR_SVC_API entity, issues the following trace event messages. The entity code assigned to FR_SVC_API events is 146.

Entity Code/Event Code **146/3**

Decimal Identifier **16814595**

Severity: Trace

Message: lapf gate created.

Meaning: The LAPF gate is created.

Entity Code/Event Code **146/4**

Decimal Identifier **16814596**

Severity: Trace

Message: lapf gate called.

Meaning: The LAPF gate has been called.

HTTP Fault Event

The HyperText Transfer Protocol service, also known as the HTTP entity, issues the following fault event message. The entity code assigned to HTTP events is 8.

Entity Code/Event Code **144/1**

Decimal Identifier **16814081**

Severity: Fault

Message: System error, service attempting restart.

Meaning: HTTP experienced a fatal error and is restarting automatically.

Action: Verify that the configuration is correct. Call the Bay Networks Technical Solutions Center if HTTP fails to restart.

HTTP Warning Events

The HyperText Transfer Protocol service, also known as the HTTP entity, issues the following warning event messages. The entity code assigned to HTTP events is 8.

Entity Code/Event Code **144/7**

Decimal Identifier **16814087**

Severity: Warning

Message: Failed to initialize HTTP Server for host <*IP_address*>, remote port <*port_no.*>.

Meaning: The HTTP Server for the indicated device and port failed to initialize.

Entity Code/Event Code **144/8**

Decimal Identifier **16814088**

Severity: Warning

Message: TCP failed to establish connection with host <*IP_address*>, remote port <*port_no.*>.

Meaning: The indicated TCP connection did not open.

Entity Code/Event Code **144/9**

Decimal Identifier **16814089**

Severity: Warning

Message: TCP transmit returned bad status code <*code*>.

Meaning: TCP transmission returned an error, indicated by the status code.

Entity Code/Event Code **144/10**

Decimal Identifier **16814090**

Severity: Warning

Message: Authorization failed (AUTH_FAILED), HTTP status: 401 Unauthorized host <*IP_address*>, port <*port_no..*>, URL '<*url*>', method '<*method*>' realm <*realm*>, user <*user*>, Referer: '<*referer*>', User-agent: '<*user_agent*>'

Meaning: The indicated user is attempting to access an entity without having appropriate access privileges. The variables identify the protected entity, the user making the attempt, the referrer, and the user agent.

Entity Code/Event Code **144/11**

Decimal Identifier **16814091**

Severity: Warning

Message: Bad msg digest (AUTH_FORGERY), HTTP status: 401 Unauthorized host <*IP_address*>, port <*port_no..*>, URL '<*url*>', method '<*method*>' realm <*realm*>, user <*user*>, Referer: '<*referer*>', User-agent: '<*user_agent*>'

Meaning: The indicated user is attempting to access an entity without having appropriate access privileges. The variables identify the protected entity, the user making the attempt, the referrer, and the user agent.

HTTP Info Events

The HyperText Transfer Protocol service, also known as the HTTP entity, issues the following info event messages. The entity code assigned to HTTP events is 8.

Entity Code/Event Code **144/2**

Decimal Identifier **16814082**

Severity: Info

Message: Protocol Initializing.

Meaning: The HTTP protocol is initializing.

Entity Code/Event Code **144/3**

Decimal Identifier **16814083**

Severity: Info

Message: Server listening for requests on local port <*port_no.*>.

Meaning: The HTTP Server is listening for requests on the indicated local port.

Entity Code/Event Code **144/4**

Decimal Identifier **16814084**

Severity: Info

Message: Server is disabled.

Meaning: The HTTP Server is not enabled.

Entity Code/Event Code **144/5**

Decimal Identifier **16814085**

Severity: Info

Message: Adding user <*user_ID*> to group <*group_ID*>.

Meaning: The specified user is being added to the indicated group.

Entity Code/Event Code **144/6**

Decimal Identifier **16814086**

Severity: Info

Message: <*message_string*>

Meaning: The message is a variable string that indicates one of several possible information messages.

HTTP Trace Events

The HyperText Transfer Protocol service, also known as the HTTP entity, issues the following trace event messages. The entity code assigned to HTTP events is 8.

Entity Code/Event Code **144/12**

Decimal Identifier **16814092**

Severity: Trace

Message: Loading archive <*archive_ID*>.

Meaning: The indicated archive is loading.

Entity Code/Event Code **144/13**

Decimal Identifier **16814093**

Severity: Trace

Message: Rejecting connection from host <*IP_address*>.

Meaning: A connection request from the indicated host has not been accepted.

Entity Code/Event Code **144/14**

Decimal Identifier **16814094**

Severity: Trace

Message: Opening connection with host <*IP_address*>, remote port <*port_no.*>.

Meaning: The HTTP server is opening a connection with the indicated host and port.

Entity Code/Event Code **144/15**

Decimal Identifier **16814095**

Severity: Trace

Message: Closing connection with host <*IP_address*>, remote port <*port_no.*>.

Meaning: HTTP is closing a connection with the indicated host and port.

Entity Code/Event Code **144/16**

Decimal Identifier **16814096**

Severity: Trace

Message: TCP aborted with status = <*code*>.

Meaning: TCP abnormally terminated for the reason code shown in this message.

Entity Code/Event Code **144/17**

Decimal Identifier **16814097**

Severity: Trace

Message: Received unexpected TCP message, type <*integer*> while in <*string*> state.

Meaning: HTTP received a TCP message unusual in this context. The variables indicate the type of message and the HTTP state.

Entity Code/Event Code **144/18**

Decimal Identifier **16814098**

Severity: Trace

Message: Bad request (BAD_REQUEST), HTTP status: 400 Bad request
host <*IP_address*>, port <*port_no..*>, URL '<*url*>', method '<*method*>'
realm <*realm*>, user <*user*>, Referer: '<*referer*>', User-agent: '<*user_agent*>'

Meaning: HTTP received an invalid request. The variables in the message indicate the source of the request, the user making the attempt, the referrer, and the user agent.

Entity Code/Event Code **144/19**

Decimal Identifier **16814099**

Severity: Trace

Message: Form data parse error (BAD_FORM), HTTP status: 400 Bad request
host <*IP_address*>, port <*port_no..*>, URL '<*url*>', method '<*method*>'
realm <*realm*>, user <*user*>, Referer: '<*referer*>', User-agent: '<*user_agent*>'

Meaning: An error occurred in parsing form data. The request is invalid. The variables in the message indicate the source of the problem, the user making the attempt, the referrer, and the user agent.

Entity Code/Event Code **144/20**

Decimal Identifier **16814100**

Severity: Trace

Message: Bad imagemap (BAD_IMAGEMAP), HTTP status: 400 Bad request
host <*IP_address*>, port <*port_no..*>, URL '<*url*>', method '<*method*>'
realm <*realm*>, user <*user*>, Referer: '<*referer*>', User-agent: '<*user_agent*>'

Meaning: A problem exists with an image map. The variables in the message indicate the source of the problem, the user making the attempt, the referrer, and the user agent.

Entity Code/Event Code **144/21**

Decimal Identifier **16814101**

Severity: Trace

Message: Archive not loaded (UNAVAILABLE), HTTP status: 503 Unavailable
host <*IP_address*>, port <*port_no..*>, URL '<*url*>', method '<*method*>'
realm <*realm*>, user <*user*>, Referer: '<*referer*>', User-agent: '<*user_agent*>'

Meaning: The requested archive is not available. The variables in the message indicate the source of the problem, the user making the attempt, the referrer, and the user agent.

Entity Code/Event Code **144/22**

Decimal Identifier **16814102**

Severity: Trace

Message: No resources (NO_RESOURCES), HTTP status: 503 Unavailable
host <*IP_address*>, port <*port_no..*>, URL '<*url*>', method '<*method*>'
realm <*realm*>, user <*user*>, Referer: '<*referer*>', User-agent: '<*user_agent*>'

Meaning: The requested resource is not available. The variables in the message indicate the source of the problem, the user making the attempt, the referrer, and the user agent.

Entity Code/Event Code **144/23**

Decimal Identifier **16814103**

Severity: Trace

Message: Unknown EWS status code <*code*>
host <*IP_address*>, port <*port_no..*>, URL '<*url*>', method '<*method*>'
realm <*realm*>, user <*user*>, Referer: '<*referer*>', User-agent: '<*user_agent*>'

Meaning: HTTP has received a nonstandard status code, indicated in the message. The variables in the message indicate the source of the problem, the user making the attempt, the referrer, and the user agent.

Entity Code/Event Code **144/24**

Decimal Identifier **16814104**

Severity: Trace

Message: Internal Error, HTTP status: 500 Internal Error
host <*IP_address*>, port <*port_no..*>, URL '<*url*>', method '<*method*>'
realm <*realm*>, user <*user*>, Referer: '<*referer*>', User-agent: '<*user_agent*>'

Meaning: An error internal to HTTP has occurred. The variables in the message indicate the source of the problem, the user making the attempt, the referrer, and the user agent.

ISDB Fault Events

The ISDB (Intelligent Serial Daughter Board) service, also known as the ISDB entity, issues the following fault event messages. The entity code assigned to ISDB events is 151.

Entity Code/Event Code **151/1**

Decimal Identifier **16815873**

Severity: Fault

Message: *<fatal_error_message>*

Meaning: The ISDB experienced a fatal error *<fatal_error_message>* and is restarting automatically.

Action: Verify that the configuration is correct. Call the Bay Networks Technical Solutions Center if the router fails to restart.

Entity Code/Event Code **151/18**

Decimal Identifier **16815890**

Severity: Fault

Message: Isdb Hardware Flash Burn Failure

Meaning: The ISDB flash burn has failed.

Action: Try to reformat the flash. If this does not work, call the Bay Networks Technical Solutions Center.

Entity Code/Event Code **151/19**

Decimal Identifier **16815891**

Severity: Fault

Message: Isdb Hardware Flash Burn Failure - Time Exceeded

Meaning: The ISDB flash burn has failed because the connection between the ISDB and the router has failed.

Action: Check that the router and the ISDB hardware are properly connected.

ISDB Warning Events

The ISDB (Intelligent Serial Daughter Board) service, also known as the ISDB entity, issues the following warning event messages. The entity code assigned to ISDB events is 151.

Entity Code/Event Code **151/2**

Decimal Identifier **16815874**

Severity: Warning

Message: *<text>*

Meaning: This is a generic warning message.

Entity Code/Event Code **151/3**

Decimal Identifier **16815875**

Severity: Warning

Message: *<Function_name>* received an unexpected buffer

Meaning: The ISDB has received buffers it should not have received. The router code is malfunctioning.

Action: The contents of the buffer will appear in the router log. Report the contents to the Bay Networks Technical Solutions Center.

Entity Code/Event Code **151/4**

Decimal Identifier **16815876**

Severity: Warning

Message: *<Function_name>* received an unexpected signal.

Meaning: The ISDB has received signals it should not have received. The router code is malfunctioning.

Action: Contact the Technical Solutions Center.

Entity Code/Event Code **151/5**

Decimal Identifier **16815877**

Severity: Warning

Message: A file *<read | write | open | seek | close>* error of type *<error_type>* has occurred.

Meaning: An read, write, open, seek, or close error of the specified type has occurred.

Action: Contact the Technical Solutions Center.

Entity Code/Event Code **151/6**
Decimal Identifier **16815878**
Severity: Warning
Message: Download/Upload operation aborted
Meaning: An ISDB download or upload operation has aborted.
Action: None

Entity Code/Event Code **151/7**
Decimal Identifier **16815879**
Severity: Warning
Message: Receive ERROR <*error_type*>
Meaning: The ISDB has received an error of the specified type.
Action: None

Entity Code/Event Code **151/20**
Decimal Identifier **16815892**
Severity: Warning
Message: Transfer Already In Progress
Meaning: An ISDB image transfer is occurring.
Action: None

Entity Code/Event Code **151/21**
Decimal Identifier **16815893**
Severity: Warning
Message: Download Attempted on Non-Present Connector
Meaning: A download of an ISDB image has been attempted on a connector that is not active.
Action: Locate the correct connector, and attach the ISDB board.

Entity Code/Event Code **151/22**

Decimal Identifier **16815894**

Severity: Warning

Message: Isdb Hardware Failure FFFFFF00 Connector *<connector_ID>*

Meaning: An ISDB hardware failure has occurred.

Action: Verify that have you installed the correct version of *ARN.exe* to support the ISDB. Verify that there is an ISDB on this slot.

ISDB Info Events

The ISDB (Intelligent Serial Daughter Board) service, also known as the ISDB entity, issues the following info event messages. The entity code assigned to ISDB events is 151.

Entity Code/Event Code **151/8**

Decimal Identifier **16815880**

Severity: Info

Message: *<text>*

Meaning: This is a generic information message.

Entity Code/Event Code **151/9**

Decimal Identifier **16815881**

Severity: Info

Message: ISDB Gate up

Meaning: The ISDB gate is up.

Entity Code/Event Code **151/10**

Decimal Identifier **16815882**

Severity: Info

Message: ISDB Gate down

Meaning: The ISDB gate is down.

Entity Code/Event Code **151/11**
Decimal Identifier **16815883**
Severity: Info
Message: Download Started
Meaning: An ISDB download has begun.

Entity Code/Event Code **151/12**
Decimal Identifier **16815884**
Severity: Info
Message: Upload Started
Meaning: An ISDB upload has begun.

Entity Code/Event Code **151/13**
Decimal Identifier **16815885**
Severity: Info
Message: Download/Upload operation complete
Meaning: The ISDB download or upload operation is complete.

Entity Code/Event Code **151/23**
Decimal Identifier **16815895**
Severity: Info
Message: Isdb Hardware Stop Connector <*connector_ID*>
Meaning: The ISDB hardware on the specified connector has stopped.

Entity Code/Event Code **151/24**
Decimal Identifier **16815896**
Severity: Info
Message: Isdb Hardware Start Connector <*connector_ID*>
Meaning: The ISDB hardware on the specified connector has started.

Entity Code/Event Code **151/25**

Decimal Identifier **16815897**

Severity: Info

Message: Isdb Hardware Flash Burn Starting

Meaning: An ISDB flash burn is starting.

Entity Code/Event Code **151/26**

Decimal Identifier **16815898**

Severity: Info

Message: Isdb Hardware Flash Burn Complete

Meaning: An ISDB flash burn is complete.

Entity Code/Event Code **151/29**

Decimal Identifier **168158101**

Severity: Info

Message: Isdb Hardware Reset Connector <*connector_ID*>

Meaning: The ISDB hardware is resetting for the specified connector.

L2TP Fault Event

The Layer 2 Tunneling protocol (L2TP) issues the following fault event message. The entity code for L2TP is 150.

Entity Code/Event Code **150/1**

Decimal Identifier **16815617**

Severity: Fault

Message: System error, service attempting restart

Meaning: L2TP experienced a fatal error. L2TP will attempt to restart automatically.

Action: Verify that the configuration is correct. Call the Bay Networks Technical Solutions Center if L2TP fails to restart.

L2TP Warning Events

The Layer 2 Tunneling protocol (L2TP) issues the following warning event messages. The entity code for L2TP is 150.

Entity Code/Event Code **150/12**

Decimal Identifier **16815628**

Severity: Warning

Message: Proxy LCP unsuccessful, SID = <*session_ID_no.*>, TID = <*tunnel_ID_no.*>

Meaning: LCP negotiations were unsuccessful.

Entity Code/Event Code **150/14**

Decimal Identifier **16815630**

Severity: Warning

Message: Failed to authenticate user <*user_name*>, SID = <*session_ID_no.*>, TID = <*tunnel_ID_no.*>

Meaning: The RADIUS server could not verify the remote user's identity.

Action: Check the RADIUS server's user name configuration.

Entity Code/Event Code **150/21**

Decimal Identifier **16815637**

Severity: Warning

Message: Max. retransmit reached. Taking down tunnel, TID <*tunnel_ID_no.*>, LAC IP: <*LAC_IP_address*>, LNS IP: <*LNS_IP_address*>

Meaning: The router has reached the maximum number of times it will retransmit data. The LNS is now disconnecting the L2TP tunnel.

Action: Try another call or try increasing the values of the Retransmit Timer, Maximum Retransmit, and Hello Timer configuration parameters.

Entity Code/Event Code **150/22**

Decimal Identifier **16815638**

Severity: Warning

Message: Retransmit buffer ring full, dropping outbound buffers, TID: <*tunnel_ID_no.*>

Meaning: Router is running low on buffer space.

Action: Increase the buffer allocation.

Entity Code/Event Code **150/23**

Decimal Identifier **16815639**

Severity: Warning

Message: The LAC has invalid Protocol Version <*version_no.*>, LAC IP: <*LAC_IP_address*>

Meaning: The LAC has the wrong L2TP software version.

Action: Update the LAC's L2TP software. Ensure that you are not running PPTP or L2F.

Entity Code/Event Code **150/24**

Decimal Identifier **16815640**

Severity: Warning

Message: <*control_message*> has invalid Framing Capabilities <*hex_value*>, LAC IP: <*LAC_IP_address*>

Meaning: The LAC requires a framing capability that the router does not support.

Action: None

Entity Code/Event Code **150/25**

Decimal Identifier **16815641**

Severity: Warning

Message: <*control_message*> has invalid Framing Type <*hex_value*>, LAC SID: <*session_ID_no.*>, TID: <*tunnel_ID_no.*>, LAC IP: <*LAC_IP_address*>.

Meaning: The LAC requires a framing type that the router does not support.

Action: None

Entity Code/Event Code **150/26**

Decimal Identifier **16815642**

Severity: Warning

Message: <*control_message*> has invalid Bearer Capabilities <*hex_value*>, LAC IP: <*LAC_IP_address*>

Meaning: The LAC requires a bearer capability that the router does not support.

Action: None

Entity Code/Event Code **150/27**

Decimal Identifier **16815643**

Severity: Warning

Message: <*control_message*> has invalid Bearer Type <*hex_value*>, LAC TID: <*tunnel_ID_no.*>, LAC IP: <*LAC_IP_address*>

Meaning: The LAC requires a bearer type that the router does not support.

Action: None

Entity Code/Event Code **150/29**

Decimal Identifier **16815645**

Severity: Warning

Message: Attempted to establish session using existing LAC SID <*session_ID_no.*>, TID <*tunnel_ID_no.*>, IP: <*LAC_IP_address*>

Meaning: The LAC is using the same session ID as an existing session.

Action: Try the call again.

Entity Code/Event Code **150/30**

Decimal Identifier **16815646**

Severity: Warning

Message: Could not find CID <*call_ID_no.*>

Meaning: The packet arrived for a session that does not exist.

Action: None

Entity Code/Event Code **150/31**

Decimal Identifier **16815647**

Severity: Warning

Message: Sequenced Payload unsupported TID <*tunnel_ID_no.*>, CID <*circuit_ID_no.*>

Meaning: The LNS asked the LAC to disable the sequenced payload. (Optional L2TP feature.)

Action: None

L2TP Info Events

The Layer 2 Tunneling protocol (L2TP) issues the following info event messages. The entity code for L2TP is 150.

Entity Code/Event Code **150/2**

Decimal Identifier **16815618**

Severity: Info

Message: L2TP Initializing

Meaning: L2TP is activating.

Entity Code/Event Code **150/3**

Decimal Identifier **16815619**

Severity: Info

Message: L2TP Down

Meaning: L2TP is not active yet.

Entity Code/Event Code **150/4**

Decimal Identifier **16815620**

Severity: Info

Message: L2TP LNS IP Address <*LNS_IP_address*> is up for slot <*slot_no.*>.

Meaning: L2TP is operating correctly on this LNS slot.

Entity Code/Event Code **150/5**

Decimal Identifier **16815621**

Severity: Info

Message: L2TP LNS IP Address <*LNS_IP_address*> is down.

Meaning: The LNS on this slot is not active.

Entity Code/Event Code **150/6**

Decimal Identifier **16815622**

Severity: Info

Message: Creating tunnel. LAC IP: <*LAC_IP_address*>, TID: <*tunnel_ID_no.*>, LNS IP: <*LNS_IP_address*>

Meaning: The router is setting up a tunnel with the specified LAC.

Entity Code/Event Code **150/7**

Decimal Identifier **16815623**

Severity: Info

Message: Tunnel established. LAC IP: <*LAC_IP_address*>, TID: <*tunnel_ID_no.*>, LNS IP: <*LNS_IP_address*>, TID: <*tunnel_ID_no.*>

Meaning: The L2TP tunnel setup is complete.

Entity Code/Event Code **150/8**

Decimal Identifier **16815624**

Severity: Info

Message: Session terminated. SID: <*session_ID_no.*>, TID: <*tunnel_ID_no.*>, LAC IP: <*LAC_IP_address*>, LNS IP: <*LNS_IP_address*>

Meaning: The L2TP session is no longer active. The user has disconnected the call at the PC, that is, there was a modem or ISDN TA hang up.

Entity Code/Event Code **150/9**

Decimal Identifier **16815625**

Severity: Info

Message: Session established. SID: <*session_ID_no.*>, TID: <*tunnel_ID_no.*>, LAC IP: <*LAC_IP_address*>, LNS IP: <*LNS_IP_address*>

Meaning: The L2TP session is active.

Entity Code/Event Code **150/13**

Decimal Identifier **16815629**

Severity: Info

Message: User <*user_name*> authenticated successfully.

Meaning: The RADIUS server authenticated the remote user successfully.

Entity Code/Event Code **150/15**

Decimal Identifier **16815631**

Severity: Info

Message: User <*user_name*> assigned address <*assigned_IP_address*> by RADIUS. (SID: <*session_ID_no.*>, TID: <*tunnel_ID_no.*>)

Meaning: The RADIUS server has assigned an IP address to the authenticated remote user.

Entity Code/Event Code **150/39**

Decimal Identifier **16815655**

Severity: Info

Message: Tunnel terminated. LAC IP: <*LAC_IP_address*>, TID: <*tunnel_ID_no.*>, LNS IP: <*LNS_IP_address*>, TID: <*tunnel_ID_no*.>

Meaning: The L2TP tunnel is terminated because the last session in the tunnel ended or the tunnel is no longer reliable, that is, no acknowledgments are received when the LNS sends a hello packet.

Entity Code/Event Code **150/40**

Decimal Identifier **16815656**

Severity: Info

Message: Session (SID: <*session_ID_no.*>, TID: <*tunnel_ID_no.*>) uses line <*line_no.*>, circuit <*circuit_no.*>

Meaning: The L2TP session is using the specified line and circuit.

Entity Code/Event Code **150/41**

Decimal Identifier **16815657**

Severity: Info

Message: User <*user_name*> assigned address <*assigned_IP_address*> by RADIUS, SID: <*session_ID_no.*>, TID: <*tunnel_ID_no.*>

Meaning: The RADIUS server assigned an IP address to the remote tunnelled user.

L2TP Trace Events

The Layer 2 Tunneling protocol (L2TP) issues the following trace event messages. The entity code for L2TP is 150.

Entity Code/Event Code **150/10**

Decimal Identifier **16815626**

Severity: Trace

Message: Skipping Proxy LCP, starting LCP renegotiation, SID = <*session_ID_no.*>, TID = <*tunnel_ID_no.*>

Meaning: The router is renegotiating LCP because the LAC did not send a proxy LCP message or does not support proxy LCP.

Entity Code/Event Code **150/11**

Decimal Identifier **16815627**

Severity: Trace

Message: Proxy LCP completed successfully, SID = <*session_ID_no.*>, TID = <*tunnel_ID_no.*>

Meaning: The router completed LCP negotiations successfully. The LCP state is now up.

Entity Code/Event Code **150/16**

Decimal Identifier **16815632**

Severity: Trace

Message: L2TP wfL2TPEntry MIB record added.

Meaning: An L2TP record has been added to the router's MIB.

Entity Code/Event Code **150/19**

Decimal Identifier **16815635**

Severity: Trace

Message: L2TP LNS failed to register with <*IP_address*>, status <*status_message*>

Meaning: L2TP LNS uses IP/UDP port 1709 and this port was unavailable.

Entity Code/Event Code **150/20**

Decimal Identifier **16815636**

Severity: Trace

Message: No Tunnel Authentication Secret

Meaning: You have not configured the router with a tunnel authentication password.

Entity Code/Event Code **150/37**

Decimal Identifier **16815653**

Severity: Trace

Message: Tunnel Authentication Successful, TID: <*tunnel_ID_no.*>, LAC IP: <*LAC_IP_address*>

Meaning: The router has completed tunnel authentication successfully with the specified LAC. L2TP sessions are now allowed from this LAC.

Entity Code/Event Code **150/8**

Decimal Identifier **16815654**

Severity: Trace

Message: Tunnel Authentication Failed, TID: <*tunnel_ID_no.*>, LAC IP: <*LAC_IP_address*>

Meaning: The router has not completed tunnel authentication with the specified LAC. The tunnel is taken down and sessions will not be accepted from this unauthorized LAC.

Entity Code/Event Code **150/57**

Decimal Identifier **16815673**

Severity: Trace

Message: No matched tunnel with TID <*tunnel_ID_no.*> found

Meaning: Packets arrived for a tunnel that does not exist.

LB Warning Event

The Learning Bridge service, also known as the LB entity, supports the following new warning message. The entity code assigned to LB events is 1.

Entity Code/Event Code **1/77**

Decimal Identifier **16777549**

Severity: Warning

Message: The interface is disabled on <*circuit_no.*> because the learning bridge base record is disabled.

Meaning: When you disable the learning bridge base record on the router, learning bridge no longer learns new bridge entries on the interface on which it is configured.

LOADER Info Events

The Dynamic Loader service, also known as the LOADER entity, issues an info message previously documented as a warning message (number 55/8). The LOADER entity also issues one new info event message (number 55/78). The entity code assigned to LOADER events is 55.

Entity Code/Event Code **55/8**

Decimal Identifier **16791304**

Severity: Info

Message: Can't find active boot image <*release_ID*>, searching volumes for another image

Meaning: The boot image that was originally booted cannot be found. The file system volume may have been moved to another slot, or the image may have been renamed.

Action: Ensure that the Dynamic Loader is able to locate the image and load all applications. If not, call the Bay Networks Technical Solutions Center.

Entity Code/Event Code **55/78**

Decimal Identifier **16791374**

Severity: Info

Message: Unloading RMONSTAT.exe because DCMMW.exe was loaded.
or:
Unloading DCMMW.exe because RMONSTAT.exe was loaded.

Meaning: The two exexutables cannot occupy memory at the same time. Loading one automatically unloads the other.

Action: None

OSPF Fault Events

The Open Shortest Path First service, also known as the OSPF entity, supports the following new fault event messages. The entity code assigned to OSPF events is 12.

Entity Code/Event Code **12/122**

Decimal Identifier **16780410**

Severity: Fault

Message: UNEXPECTED DEATH of MSPF gate new_gh 0x%08x for area <*area*>.

Meaning: MOSPF experienced an internal inconsistency while performing the multicast OSPF calculations. OSPF is restarting automatically. OSPF will attempt to restart up to five times.

Action: Call the Bay Networks Technical Solutions Center if OSPF fails to restart.

Entity Code/Event Code **12/123**

Decimal Identifier **16780411**

Severity: Fault

Message: UNEXPECTED DEATH of MOSPF_LSA gate new_gh 0x%08x.

Meaning: MOSPF experienced a fatal error and is restarting automatically. OSPF will attempt to restart up to five times.

Action: Call the Bay Networks Technical Solutions Center if OSPF fails to restart.

OSPF Warning Events

The Open Shortest Path First service, also known as the OSPF entity, supports the following new warning event messages. The entity code assigned to OSPF events is 12.

Entity Code/Event Code **12/121**

Decimal Identifier **16780409**

Severity: Warning

Message: Invalid MOSPF configuration: wfOspfMulticastExtensions == 0x%08x.

Meaning: The configured value for the OSPF Global Multicast Extensions parameter was illegal.

Action: Set the OSPF Global Multicast Extensions parameter to the appropriate value, 0 (no multicast forwarding is enabled), 1 (intra-area multicasting only), 3 (intra-area and inter-area multicasting), 5 (intra-area and inter-AS multicasting), or 7 (intra-area, inter-area, and inter-AS multicasting).

Entity Code/Event Code **12/124**

Decimal Identifier **16780412**

Severity: Warning

Message: MTU from <*neighbor_address*> on interface <*local_address*> too large, dropping DD packet.

Meaning: The neighbor's MTU size configured for the interface is larger than the MTU size configured for the local interface.

Action: An adjacency is not established with this neighbor. OSPF packets that exceed the local interface MTU will be lost, possibly effecting assimilation and causing flooding of Link State Advertisements.

OSPF Info Event

The Open Shortest Path First service, also known as the OSPF entity, supports the following new info event message. The entity code assigned to OSPF events is 12.

Entity Code/Event Code **12/125**

Decimal Identifier **16780413**

Severity: Info

Message: %s interface <*local_address*> received duplicate DD packet from <*neighbor_address*>.

Meaning: A duplicate Database Description packet was received from the specified neighbor on the specified interface.

Action: The duplicate packet is ignored.

PPP Warning Events

The Point-to-Point service, also known as the PPP entity, supports the following new warning event messages. The entity code assigned to PPP events is 44.

Entity Code/Event Code **44/232**

Decimal Identifier **16788712**

Severity: Warning

Message: Received attribute value pair with incorrect length, session ID number = <*session_ID_no.*>, tunnel ID number = <*tunnel_ID_no.*>

Meaning: The router received an attribute value pair, session ID number and tunnel ID number, with an incorrect length.

Action: Make sure that the session ID number and tunnel ID number use the correct format.

Entity Code/Event Code **44/233**

Decimal Identifier **16788713**

Severity: Warning

Message: Proxy link control protocol unsuccessful on <*control_message*> attribute value pair, session ID number = <*session_ID_no.*>, tunnel ID number = <*tunnel_ID_no.*>, renegotiating link control protocol.

Meaning: The router failed to negotiate its link control protocol due to <*control_message*> attribute value pair. The router will now renegotiate its link control protocol.

RFWALL Warning Events

The FireWall service, also known as the RFWALL entity, supports the following revised warning event messages. The entity code assigned to RFWALL events is 119.

Entity Code/Event Code **119/27**

Decimal Identifier **16807707**

Severity: Warning

Message: fw_skey_getkey_client: <*IP_address*> not found

Meaning: The router's IP address could not be found inside NVRAM during a get operation.

Action: Reissue the **skey** command.

Entity Code/Event Code **119/28**

Decimal Identifier **16807708**

Severity: Warning

Message: fw_skey_changekey_client: <<*IP_address*> not found

Meaning: The router's IP address could not be found inside NVRAM during a changekey operation.

Action: Reissue the **skey** command.

Entity Code/Event Code **119/31**

Decimal Identifier **16807711**

Severity: Warning

Message: fw_skey_getkey_server: <*IP_address*> not found

Meaning: The IP address of the firewall management station could not be found inside NVRAM during a get operation.

Meaning: None

RFWALL Info Events

The FireWall service, also known as the RFWALL entity, supports the following revised info event messages. The entity code assigned to RFWALL events is 119.

Entity Code/Event Code **119/37**
Decimal Identifier **16807717**
Severity: Info
Message: FWALLC initializing.
Meaning: Firewall is initializing. This is a normal firewall state during boot or reboot.

Entity Code/Event Code **119/97**
Decimal Identifier **16807776**
Severity: Info
Message: FIREWALL FILTER DOWNLOAD COMPLETE ON: line <*line_no.*>.
Meaning: Filter has been downloaded successfully on the specified line.

Entity Code/Event Code **119/116**
Decimal Identifier **16807796**
Severity: Info
Message: DP: Couldn't find firewall instance to delete for slot <*slot_no.*>, <*port_no.*>.
Meaning: Could not delete firewall because it could not be found on slot <*slot_no.*>, <*port_no.*>.

RFWALL Trace Event

The FireWall service, also known as the RFWALL entity, supports the following revised trace event message. The entity code assigned to RFWALL events is 119.

Entity Code/Event Code **119/99**
Decimal Identifier **16807778**
Severity: Trace
Message: FWALLC, IF_CHG_MSG: Line = <*line_no.*>, STATE = <*state*>
Meaning: State trace message.

RMONSTAT Info Events

The RMONSTAT service, also known as the RMONSTAT entity, issues the following info event messages. The entity code assigned to RMONSTAT events is 154.

Entity Code/Event Code **154/17**

Decimal Identifier **16816666**

Severity: Info

Message: RMONSTAT_IF_FAILURE

Meaning: The RMONStat subagent was unable to determine the interface number for the Ethernet interface. This condition is likely to occur when you attempt to load the RMONStat subsystem before you configure an Ethernet interface on the router.

Action: Configure an Ethernet interface before you configure the RMONStat subagent on the router.

Entity Code/Event Code **154/18**

Decimal Identifier **16816667**

Severity: Info

Message: RMONSTAT_DATA_RESET

Meaning: The Ethernet controller has been reset on the router. This resets the RMON counters and deletes the accumulative history table on the ARN 100 router.

STAC Fault Event

The STAC LZS compression protocol issues the following fault event message. The entity code is 142.

Entity Code/Event Code **142/1**

Decimal Identifier **16813569**

Severity: Fault

Message: System error, service attempting restart.

Meaning: Stac LZS experienced a fatal error. Stac LZS will attempt to restart automatically.

Action: Verify that the configuration is correct. Call the Bay Networks Technical Solutions Center if Stac LZS fails to restart.

STAC Warning Events

The STAC LZS compression protocol issues the following warning event messages. The entity code is 142.

Entity Code/Event Code **142/2**

Decimal Identifier **16813570**

Severity: Warning

Message: Maximum number of wfStacCircuitEntry reached. Ignoring entry.

Meaning: The maximum number of Stac LZS interfaces have been configured. You cannot add any more.

Action: Verify that the number of Stac LZS circuits does not exceed 1024.

Entity Code/Event Code **142/3**

Decimal Identifier **16813571**

Severity: Warning

Message: Invalid compression mode. Using default value.

Meaning: You have configured a compression mode that Stac LZS does not support.

Action: Accept the default compression mode, which is mode 3.

Entity Code/Event Code **142/4**

Decimal Identifier **16813572**

Severity: Warning

Message: Invalid engine type. Using default value.

Meaning: You have tried to configure a compression engine type (software or hardware) that is not valid for this interface.

Action: Accept the default engine type.

Entity Code/Event Code **142/5**

Decimal Identifier **16813573**

Severity: Warning

Message: Engine Registration failed for circuit <*circuit_no.*> compression down.

Meaning: The compression engine registration did not complete.

Action: None

Entity Code/Event Code **142/6**

Decimal Identifier **16813574**

Severity: Warning

Message: CCP Registration failed for circuit <*circuit_no*.> compression down on this circuit.

Meaning: Stac LZS CCP registration did not complete successfully.

Action: None

STAC Info Events

The STAC LZS compression protocol issues the following info event messages. The entity code is 142.

Entity Code/Event Code **142/7**

Decimal Identifier **16813575**

Severity: Info

Message: Service initializing.

Meaning: Stac LZS is initializing.

Entity Code/Event Code **142/8**

Decimal Identifier **16813576**

Severity: Info

Message: Service is up.

Meaning: Stac LZS service is active.

Entity Code/Event Code **142/9**

Decimal Identifier **16813577**

Severity: Info

Message: Attempt to connect circuit <*circuit_no*> has timed out.

Meaning: The router did not activate the circuit in the specified time period.

Entity Code/Event Code **142/10**

Decimal Identifier **16813578**

Severity: Info

Message: Attempt to disconnect circuit <*circuit_no*> has timed out.

Meaning: The router did not disconnect the circuit in the specified time period.

STAC Trace Event

The STAC LZS compression protocol issues the following trace event message. The entity code is 142.

Entity Code/Event Code **142/11**

Decimal Identifier **16813579**

Severity: Trace

Message: Sequence # error: Expected seq. #: = <*sequence_no.*> Rcvd seq. # = <*sequence_no*>. Sequence # mismatch, Reset cir: <*circuit_no.*>

Meaning: The decompressor has detected an error, for example an expected sequence number did not match the received sequence number. The local decompression history and the sender's compression history has to be reset.

TELNET Fault Event

The Telnet Server service, also known as the TELNET entity, issues the following fault event message. The message contains corrected Decimal Identifiers. The entity code assigned to TELNET events is 40.

Entity Code/Event Code **40/1**

Decimal Identifier **16787457**

Severity: Fault

Message: System error, service attempting restart.

Meaning: The Telnet application utility experienced a fatal error and is restarting automatically. Telnet will attempt to restart up to five times.

Action: Verify that the configuration is correct. Call the Bay Networks Technical Solutions Center if Telnet fails to restart.

TELNET Warning Events

The Telnet Server service, also known as the TELNET entity, issues the following warning event message. The message contains corrected Decimal Identifiers. The entity code assigned to TELNET events is 40.

Entity Code/Event Code **40/2**

Decimal Identifier **16787458**

Severity: Warning

Message: Missing Telnet configuration record -- Disabled.

Meaning: Telnet is not configured for the router platform.

Action: Configure Telnet, if desired.

TELNET Info Events

The Telnet Server service, also known as the TELNET entity, issues the following info event messages. The messages contain corrected Decimal Identifiers. The entity code assigned to TELNET events is 40.

Entity Code/Event Code **40/3**

Decimal Identifier **16787459**

Severity: Info

Message: Connection Manager received connection request from <*client_IP_address*>

Meaning: The client identified by <*IP_address*> is attempting to establish a Telnet connection with the Technician Interface.

Entity Code/Event Code **40/4**

Decimal Identifier **16787460**

Severity: Info

Message: Connection Manager initializing.

Meaning: The Telnet server is initializing.

Entity Code/Event Code **40/5**

Decimal Identifier **16787461**

Severity: Info

Message: Connection Manager listening on TCP port <*Telnet_port_no.*>

Meaning: The Telnet server is ready to receive client connections on the specified TCP port.

Entity Code/Event Code **40/6**

Decimal Identifier **16787462**

Severity: Info

Message: Connection Manager down. Awaiting TELNET enable.

Meaning: Telnet is not enabled for the router platform.

Action: Enable the Telnet server to process incoming client requests.

Entity Code/Event Code **40/7**

Decimal Identifier **16787463**

Severity: Info

Message: Connection manager down. Awaiting TELNET Configuration.

Meaning: Telnet is not configured for the router platform.

Action: Configure the Telnet server to process incoming client requests.

Entity Code/Event Code **40/8**

Decimal Identifier **16787464**

Severity: Info

Message: Connection manager down. Awaiting TCP Enable.

Meaning: TCP is not enabled for the router platform.

Action: Enable TCP (and the Telnet server) to process incoming client requests.

Entity Code/Event Code **40/9**

Decimal Identifier **16787465**

Severity: Info

Message: Session Manager initializing.

Meaning: A Telnet connection is being established.

Entity Code/Event Code **40/10**

Decimal Identifier **16787466**

Severity: Info

Message: Session Manager terminating for <*client_IP_address*> <*client_port_no.*> connection.

Meaning: The Telnet session specified by <*client_IP_address*> and <*client_port_no.*> is terminating.

Entity Code/Event Code **40/11**

Decimal Identifier **16787467**

Severity: Info

Message: Session Manager up for <*client_IP_address*> <*client_port_no.*> connection.

Meaning: The Telnet session specified by <*client_IP_address*> and <*client_port_no.*> is ready.

Entity Code/Event Code **40/12**

Decimal Identifier **16787468**

Severity: Info

Message: Session Manager down for <*client_IP_address*> <*client_port_no.*> connection.

Meaning: The Telnet session specified by <*client_IP_address*> and <*client_port_no.*> is disabled.

Entity Code/Event Code **40/13**

Decimal Identifier **16787469**

Severity: Info

Message: State of TELNET MIB object changed; restarting

Meaning: The Telnet MIB has been reconfigured. All Telnet sessions are being terminated.

Entity Code/Event Code **40/14**

Decimal Identifier **16787470**

Severity: Info

Message: TELNET MIB attribute update signal received.

Meaning: The MIB attribute changed. The change is effective for the following Telnet session.

TELNET Trace Events

The Telnet Server service, also known as the TELNET entity, issues the following trace event messages. The messages contain corrected Decimal Identifiers. The entity code assigned to TELNET events is 40.

Entity Code/Event Code **40/15**

Decimal Identifier **16787471**

Severity: Trace

Message: Connection manager refused connection from <*client_IP_address*> <*client_port_no.*>. State: <*state*>.

Meaning: A request for a Telnet session has been rejected due to insufficient system resources.

Entity Code/Event Code **40/16**

Decimal Identifier **16787472**

Severity: Trace

Message: Remote session from <*client_IP_address*> <*client_port_no.*> disconnected.

Meaning: The Telnet session has been terminated.

Entity Code/Event Code **40/17**

Decimal Identifier **16787473**

Severity: Trace

Message: Session Manager flow control failed, input queue overflow.

Meaning: An internal error occurred.

VCCT Fault Event

The virtual circuit service for DLSw/APPN Boundary functionality, also known as the VCCT entity, issues the following fault event message. The entity code assigned to VCCT events is 153.

Entity Code/Event Code **153/1**

Decimal Identifier **16816385**

Severity: Fault

Message: System error, service attempting restart.

Meaning: VCCT experienced a fatal error and is restarting automatically.

Action: Verify that the configuration is correct. Contact the Bay Networks Technical Solutions Center if this condition persists.

X.25 PAD Fault Event

The X.25 PAD service, also known as the X.25 PAD entity, issues the following fault event message. The entity code assigned to X.25 PAD events is 152.

Entity Code/Event Code **152/1**

Decimal Identifier **16816129**

Severity: Fault

Message: X.25 PAD Error: <*fatal_error_message*>

Meaning: The router experienced a fatal error <*fatal_error_message*> and is restarting automatically. The router will attempt to restart up to five times.

Action: Verify that the configuration is correct. Call the Bay Networks Technical Solutions Center if the router fails to restart.

X.25 PAD Warning Events

The X.25 PAD service, also known as the X.25 PAD entity, issues the following warning event messages. The entity code assigned to X.25 PAD events is 152.

Entity Code/Event Code **152/2**

Decimal Identifier **16816130**

Severity: Warning

Message: *<text>*

Meaning: This is a generic warning message.

Action: None

Entity Code/Event Code **152/3**

Decimal Identifier **16816131**

Severity: Warning

Message: *<Function>* received an unexpected buffer

Meaning: The PAD has received buffers it should not have received. The router code is malfunctioning.

Action: The contents of the buffer will appear in the router log. Report the contents to the Bay Networks Technical Solutions Center.

Entity Code/Event Code **152/4**

Decimal Identifier **16816132**

Severity: Warning

Message: *<Function_name>* received an unexpected signal.

Meaning: The PAD has received signals it should not have received. The router code is malfunctioning.

Action: Contact the Technical Solutions Center.

X.25 PAD Info Event

The X.25 PAD service, also known as the X.25 PAD entity, issues the following info event message. The entity code assigned to X.25 PAD events is 152.

Entity Code/Event Code **152/5**

Decimal Identifier **16816133**

Severity: Info

Message: *<text>*

Meaning: This is a generic information message.

Action: None

X.25 PAD Trace Event

The X.25 PAD service, also known as the X.25 PAD entity, issues the following Trace event message. The entity code assigned to X.25 PAD events is 152.

Entity Code/Event Code **152/6**

Decimal Identifier **16816134**

Severity: Trace

Message: *<text>*

Meaning: This is a generic trace message.

Mananging Your Network Using the HTTP Server

The following section is an amendment to *Managing Your Network Using the HTTP Server.*

Viewing HTTP Statistics Using Statistics Manager

On page B-5, Figure B-5, "HTTP Server Configuration Window," the entry in the State column should be "enabled" instead of "enable."

Troubleshooting Routers

The following section is an amendment to *Troubleshooting Routers*.

Troubleshooting an FT1 Connection

This section assumes that you have isolated a problem to a multichannel T1 (FT1) connection. If not, refer to Chapter 2 in *Troubleshooting Routers* to determine whether these instructions apply to your problem.

To troubleshoot an FT1 connection:

1. **Filter the log to display only messages from the FT1 entity running on the slots experiencing the problem.**

   The Technician Interface command is as follows:

   log -fftwid -eDS1E1 -s*<slot_no.>*

   Example

   If you are filtering events from slot 1, enter the following command:

   log -fftwid -eDS1E1 -s1

Note: The ARN, AN, and ANH are single channel so only one FT1 slot is available on these modules.

2. **Check the following FT1 MIB entries by entering the following Technician Interface commands:**

   get wfDrivers.14.0
   get wfLinkModules.17.0

   Or, use this Quick Get path: wfSoftwareConfig > wfLinkModules > wfQssyncLoad.

3. **Make sure that the Line Type and Line Coding supplied by the T1 provider match the associated settings in the FT1 configuration.**

4. **Make sure that the digital signal, level 0 (DS0) channels match at both the router and the central office.**

5. **Watch the LEDs on the back of the FT1 module. If the Sync LED keeps flashing, the line build out (LBO) is not in sync. This indicates impedance or resistance on the line. Ask the T1 carrier if you should set it to long haul or short haul, and configure the LBO parameter accordingly.**

   The Sync LED stays on when the framer is in sync with the carrier's clock.

6. **Make sure that you set the LBO appropriately.**

   For example, 0.0 dB is short haul (up to 133 ft).

7. **Use the FT1 built-in bit error rate test (BERT) and line loop-up, loop-down, and payload loopbacks for troubleshooting. (This feature is available only with Site Manager in dynamic mode.)**

   Note that only one port can be in BERT mode at a time.

   Payload loopbacks are available in extended super frame (ESF) line type mode only.

8. **Make sure that the clocking is set to Internal or Port1 Ext Loop. These settings are equivalent to Sync External.**

   The internal clocking of the FT1 link module is the same as the internal clocking of the T1 link module.

9. **Make sure that the CRC16 (cyclic redundancy check) or CRC32 match the carrier's specifications.**

10. **Make sure that the value of the Inter Frame Time Fill parameter matches idles (0xFF) or flags (0x7E) with the remote end of the link.**

11. **Check the events from the entity DS1E1 (multichannel T1/E1 driver service) to view the FT1 log events.**

    FT1 uses the wfDS1E1 MIB entries. Therefore, the entity name associated with FT1 is DS1E1, *not* FT1.

    FT1 uses the wfSyncEntry object; T1 uses the wfLogicalLineEntry object.

Upgrading Routers from Version 7-11.xx to Version 12.00

The following section is an amendment to *Upgrading Routers from Version 7-11.xx to Version 12.00.*

BOOT and Diagnostic PROM Upgrades for Version 12.10

Table 3 shows the routers that require a new version of boot and diagnostic PROMs for BayRS Version 12.10. Upgrade the PROMs if the features you need depend on a PROM version more recent than the version now in your router.

Table 3. Boot and Diagnostic PROMs for BayRS Version 12.10

Router Model	Boot PROM Version	Boot PROM File Name	Reason for Upgrading PROM	Diagnostic PROM File Name	Diagnostic PROM Version
AN	9.00c	*anboot.exe*	New hardware platform support	*andiag.exe*	V7.30
AN200	11.01	*an200boot.exe*	New hardware platform support	*an200diag.exe*	V1.00
ARE (BN)	11.02	*areboot.ppc*	New hardware platform support	*arediag.ppc*	V1.16
ARE s5000	12.10	*s5000boot.exe*	N/A	*S5000diag.ppc*	V1.16
ARN	V1.18	*arnboot.exe*	Support for ARN platform and miscellaneous bug fixes	*arndiag.exe*	V2.00
ARN_PDBROM.ROM	-----	------	Support for PDB diagnostics for the ARN platform	*arndiag.exe*	V1.06
ASN™	10.00	*asnboot.exe*	N/A	*asndiag.exe*	V2.24
BN®	8.10	*freboot.exe*	N/A	*frediag.exe*	V4.12
ARE s5000	11.00	*s5000boot.exe*	N/A	*S5000diag.exe*	V0.04

Using the Bay Command Console (AN/BN Routers)

The following sections are amendments to *Using the Bay Command Console (AN/BN Routers)*:

- Obtaining the Version of a Help File on a Router
- Help updates

Obtaining the Version of a Help File on a Router

So that you can determine if you have the correct and latest version of the BCC Help file *bcc.help* loaded on your AN/BN router, you can enter the following command at any BCC prompt:

help-file-version

Example:

```
box# help-file-version
Help file 2:bcc.help, contains this version data:
  Data version is:    2.
  Creation date is:   1997 Nov 20 14:42:40 hrs.
```

If a later version of *bcc.help* exists for this release, you can use a Web browser to obtain it from the following Bay Networks URL:

http://support.baynetworks.com/Library/tpubs/bcc

Follow the instructions at this Web site to obtain a copy of the BCC Help file you need.

Help Updates

We made minor revisions in the following BCC **help** [*<option>*] commands:

Command	Command Input/Output Revisions
help **help -more**	• Added information about the new **help-file-version** command • Made the information sequence and content more consistent between the output of the **help** and **help -more** commands
help commands **help commands -more**	• Added information on the new **help-file-version** command • Removed information on the **!** command, which is valid only at the Technician Interface prompt
help delete	• Corrected the sequence of step numbering in the example BCC **delete** procedure
help parameters ip	• Added definitions for two parameters, **routing-table-indexes** and **routing-table-deviation** • Removed the definition for the **mib-table** parameter, which is obsolete in this version of the BCC interface
help parameters telnet	• Removed the definition for **state** parameter, which is invalid for the BCC **telnet** object
help parameters ip bgp announce match as	• Changed the name of the **as** object to **inbound-as**, which in turn changed the **help parameters** command for this object to **help parameters ip bgp announce match inbound-as**
help parameters ip bgp announce match peer	• Changed the name of the **peer** object to **inbound-peer**, which in turn changed the **help parameters** command for this object to **help parameters ip bgp announce match inbound-peer**
help tree **help tree ip**	• Changed the name of the **as** and **peer** objects configurable in the **ip bgp announce match** context to **inbound-as** and **inbound-peer**, respectively. These changes appear in the 12.10 version of the router configuration tree displayed by the **help tree** and **help tree ip** commands.

Using Technician Interface Scripts

The following entities have new or amendned sections in *Using Technician Interface Scripts.*

Show commands:

- AHB
- FR
- FWALL
- L2TP
- LANE LES
- MOSPF
- OSPF
- PPP
- SR
- STAC
- SYNC

Show *<entity_name>* **version** commands:

All entities display the following message in response to the **show** *<entity_name>* **version** command:

```
<entity_name>.bat Release 12.10
```

Enable/disable commands:

- STAC

Deleted command:

The **show dvmrp stats vifs** command has been removed from BayRS 12.10.

show ahb

The **show ahb** *<option>* commands display information about the ATM Half-Bridge (AHB) protocol. For detailed information on the Bay Networks implementation of AHB, see *Configuring ATM Half-Bridge Services*.

The **show ahb** command supports the following subcommand options:

base
circuits
hosts [<slot> <cctnum> <vpi> <vci> <addr>]
routes
stats

base

Displays AHB global parameters. This is the base record for the AHB protocol and controls the protocol for the entire system.

Sample Display – show ahb base

```
Protocol  : AHB
Forwarding Mode : Enabled
Inbound Filtering: Disabled
Learn Method: secure
Debug Level: 5
```

The columns displayed have the following meanings:

Protocol	Name of protocol, in this case AHB.
Forwarding Mode	Indicates the state of AHB packet forwarding (enabled or disabled).
Inbound Filtering	Indicates that inbound packet filtering is enabled on the AHB router.

Learn Method	Method by which AHB automatically learns new bridge entries on the AHB router. You can configure AHB in one of the following learning methods: • Secure • Unsecure • Both • None
Debug Level	Indicates the level of debug messaging you want the AHB router to display in its log file.

circuits

Displays circuit and state information for all AHB circuits.

Sample Display – show ahb circuit

```
Circuit       Num  Status  Proxy Arp  Def Subnet Mask
---------------  ---  ------  ---------  -----------
ATMSR_1413101.4     4  Up      Enabled    0.0.0.0
```

The columns displayed have the following meanings:

Circuit	Name of the circuit on which you configured AHB.
Num	Number of the circuit on which you configured AHB.
Status	Current state of the AHB protocol: Not Present (enabled but not yet started), or Up.
Proxy Arp	Indicates whether proxy ARP is enabled or disabled on the AHB router. If enabled, the AHB router responds to ARP requests sent from ATM-attached hosts with its own hardware address as the target MAC address. If disabled, the AHB ignores ARP requests sent from ATM-attached hosts.
Def Subnet Mask	IP subnet mask for host entries learned unsecurely.

hosts [*<slot> <cctnum> <vpi> <vci> <addr>*]

Displays the base record information for AHB. The base record controls AHB for the entire system.

<slot>	Shows only hosts on the specified slot
<*cctnum*>	Shows only hosts on the specified circuit
<*vpi*>	Shows only hosts on the specified VPI
<*vci*>	Shows only hosts on the specified VCI
<*addr*>	Shows only hosts with the specified IP address

Sample Display – show ahb hosts

```
Slt Host Addr      Subnet         Cct VPI  VCI  Fl TxPkts   RxPkts
--- ---------------- -------------------- ---------------- --- ----
13  2.2.2.27       255.0.0.0      4   0    100 2 1 11
```

The columns displayed have the following meanings:

Slt	Indicates the slot on which the AHB router learned the CPE host address.
Host Addr	IP address of the CPE host that sends packets to the AHB router.
Subnet	Subnet mask of the CPE host.
Cct	Circuit number on which AHB is configured on the router.
VPI	Indicates the virtual path of the PVC configured on the ATM inteface. The VPI is part of the cell header, which can contain a maximum of 8 VPI bits.
VCI	Identifies the virtual channel of the PVC configured on the ATM interface. The VCI is part of the cell header, which can contain a maximum of 16 VCI bits.
F1	Indicates “Flags” field: 0x2= host learned dynamically 0x10=disabling forwarding to/from host 0x20= host learned in unsecure mode

TxPkts	Number of packets the router transmits to the CPE host at the remote site.
RxPkts	Number of packets the router receives from the CPE host at the remote site.

routes

Displays information from the AHB routing table.

Sample Display – show abh routes

```
Destination        Mask       Proto   Age      Cost     NextHop Addr /  AS
--------------- --------------- ----- -------- --------
4.0.0.0         255.0.0.0       AHB   19       1         0.0.0.4
1 route(s) found
```

The columns displayed have the following meanings:

Destination	Destination IP address for this route. 0.0.0.0 indicates a default route.
Mask	Subnet mask to be combined with the destination address and then compared with the value in Destination. If the value of Destination is 0.0.0.0 (a default route), then the value of Mask is also 0.0.0.0.
Proto	Routing method through which the router learned this route: Other, Local, Netmgmt, ICMP, EGP, GGP, Hello, RIP, IS-IS, OSPF, or BGP.
Age	Number of seconds since this route was last updated or verified to be correct. The meaning of “too old” depends on the routing protocol specified under Proto.
Cost	Number of hops to reach the destination.
NextHop Addr/AS	IP address of the next hop and next Autonomous System of this route. If the next hop is an unnumbered interface, the command displays 0.0.0.*n*, where *n* is the number of the circuit on which the interface has been configured.

stats

Displays all AHB statistics for each circuit.

Sample Display – show ahb stats

```
AHB Statistics: Tot Nets = 4, Tot Hosts = 1, State = Enabled

Incoming Pkts: Total =      15392  Fwd'd =       7962
Outgoing Pkts: Total =         11  Fwd'd =       7389  Unknown = 0

CCT    TxPkts      TxDrop      RxPkts      RxDrop
---  ----------  ----------  ----------  ----------
  4        7389           0       15392          35
```

The fields displayed have the following meanings:

Tot Nets	The total number of networks in the AHB configuration.
Tot Hosts	The total number of hosts configured on the network.
State	The current state of the AHB protocol: Disabled (manually disabled), Down, Init (Initializing), Not Present (enabled but not yet started, or Up.
Incoming Pkts	The total number of packets that the AHB router receives from the IP routed network.
Outgoing Pkts	The total number of outgoing packets that the AHB router transmits to the IP routed network.
CCT	The total number of circuits configured for AHB.
TxPkts	The total number of packets transmitted by the AHB router.
TxDrop	The total number of packets dropped by the AHB router.
RxPkts	The total number of packets that the AHB router receives from CPE hosts.
RxDrop	The total number of packets that the router drops because they are not contained in the bridge table.

show fr

The **show fr** *<option>* commands display configuration, state, and statistical information about Frame Relay services. For details on the Bay Networks implementation of Frame Relay services, see *Configuring Frame Relay Services.*

The **show fr** command supports new options for the following subcommands:

pt <options>	svcs <options>
stats lapf <options>	vcs [<line> | <line.llindex> | <line.llindex.DLCI>]
stats signalling <options>	

pt *<options>*

Displays PVC pass through statistics for all PVCs or for a specified PVC.

The **show fr pt** command includes the following subcommand options:

- stat
- map

The table includes the following information, depending on the subcommand option:

Circuit name	Identifies the circuit.
DLCI	Identifies the DLCI.
Rx Frames	Number of frames received.
Tx Frames	Number of frames transmitted.
Discards	Number of frames discarded.
Drops	Number of frames dropped.
State	State of the connection.
Circuit name (A) Cct (A) DLCI (A)	Identifies the first circuit in a pass through mapping.
Cct Name (B) Cct (B) DLCI (B)	Identifies the second circuit in a pass through mapping.

Sample Display - show fr pt stat

```
1:1]$ sho fr pt stat
Cct Name        DLCI   RxFrames  TxFrames  Discards  Drops     State
--------------- ------ --------- --------- --------- --------- ---------
201404.0.6      101        66365     68967         0         0 Active
201403.0.10     201        68967     66365         0         0 Active
2 entries found
```

Sample Display - show fr pt map

```
[1:1]$ sho fr pt map
Cct Name(A)     Cct(A) DLCI(A)  Cct Name(B)     Cct(B) DLCI(B) State
--------------- ------ ------   --------------- ------ ------  ---------
201404.0.6      6      101      201403.0.10     10     201     Active
1 entry found
```

stats lapf *<options>*

Displays LAPF statistics for all VCs or for a specified VC. These messages conform to ITU-T Recommendation Q.921, *Digital Subscriber Signalling System No. 1 (DSS 1) -ISDN User-Network Interface, Data Link Layer Specification*, March 1993.

The **show fr lapf** command includes the following subcommand options:

- errors
- receive
- traffic
- transmit

The table includes the following information, depending on the subcommand option:

Line.LLIndex.DLCI	Line or instance identifier for the service record.
Window	Number of unacknowledged frames that LAPF can send before receiving an acknowledgment.
SABME	Number of SABME (Set Asynchronous Balanced Mode Extended) commands sent. SABME frames start multiple frame operation.

UA	Unnumbered Acknowledgment messages sent. If a station that receives a SABME or DISC command is able to execute the command, it responds with a UA.
DISC	Disconnect command; releases multiple frame operation.
DM	Disconnected Mode, which indicates collision of commands and responses, with the consequence that multiple frame operation cannot execute.
FRMR	Frame reject errors that cannot be recovered by retransmitting an information frame.
REJ	Reject messages, which request retransmission of information frames.
RNR	Receive Not Ready messages, indicating information frames received when the receiving station was temporarily busy.
RR	Receive Ready frames. These are sent if the station is ready to receive information frames, to adknowledge previously received information frames, and to clear a previous busy condition.
XID	Exchange ID messages, which convey station identification information.
Retransmit Timer Expiry Status (T200)	Number of times the T200 timer has expired.
Idle Time Expiry (T203)	Number of times the T203 timer has expired.
Retransmit Limit Exceeded (N200)	Number of times the N200 retransmit limit has been exceeded.
Frame Size Exceeded (N201)	Number of times the N200 frame size limit has been exceeded.
Unnumbered Info Frames Sent	Count of unnumbered information frames sent.
Numbered Info Frames Sent	Count of numbered information frames sent.
Unnumbered Info Frames Received	Count of unnumbered information frames received.
Numbered Info Frames Received	Count of numbered information frames received.

Sample Display - show fr stats lapf receive

```
[4:1]$ show fr stats lapf receive

Line.LLIndex Window SABME  UA   DISC   DM   FRMR   REJ   RNR   RR    XID
------------ ------ ----- ----- ----- ----- ----- ----- ----- ----- -----
204101.0          7     1     1     0     0     0     0     0     2     0
1 entry found
```

Sample Display - show fr stats lapf transmit

```
4:1]$ show fr stats lapf transmit

Line.LLIndex Window SABME  UA   DISC   DM   FRMR   REJ   RNR   RR    XID
------------ ------ ----- ----- ----- ----- ----- ----- ----- ----- -----
204101.0          7     1     1     0     0     0     0     0     3     0
1 entry found
```

Sample Display - show fr stats lapf errors

```
[4:1]$ show fr stats lapf errors

                     Retransmit   Idle Timer Retransmit     Frame Size
                     Timer Expiry Expiry     Limit Exceeded Exceeded
Line.LLIndex Status  (T200)       (T203)     (N200)         (N201)
------------ -------- ------------ ---------- -------------- ----------
204101.0     Running             0          0              0          0
1 entry found
```

Sample Display - show fr stats lapf traffic

```
[4:1]$ show fr stats lapf traffic

                     ---------Sent---------- --------Received-------
                     Unnumbered  Numbered    Unnumbered  Numbered
Line.LLIndex Status  Info Frames Info Frames Info Frames Info Frames
------------ -------- ----------- ----------- ----------- -----------
204101.0     Running           0          10           2
1 entry found
```

stats signalling *<options>*

Displays signalling statistics for all VCs or for a specified VC. These messages conform to ITU-T Recommendation Q.931, *Digital Subscriber Signalling System No.1 (DSS1) - ISDN User-Network Interface, Layer 3 Specification for Basic Call Control*, March 1993.

The **show fr signalling** command includes the following subcommand options:

- receive
- transmit

The table includes the following information, depending on the subcommand option:

Line.LLIndex.DLCI	Line or instance identifier for the service record.
Call setup	Number of call setups between the calling user and the network to initiate a call.
Call proceed	Number of calls between the calling user and the network to indicate requested call establishment has begun.
Connect	Number of calls between the calling user and the network to indicate call acceptance by the called user.
Disconnect	Number of calls by the calling user to request the network to clear an end-to-end connection, or by the network to indicate that the connection is cleared.
Release	Number of messages between the calling user and the network to indicate that the sender has disconnected the call.
Release Complete	Number of messages between the calling user and the network to indicate that the sender has released the call reference.
Status	Number of messages between the calling user and the network to report error conditions.
Status Enquiry	Number of messages between the calling user and the network to solicit a Status message.

Sample Display - show fr stats signalling receive

```
4:1]$ show fr stats signalling receive

                  Call                                Release        Status
Line.LLIndex Setup Proceed Connect Disconnect Release Complete Status
Enquiry
------------ ----- ------- ------- ---------- ------- -------- ------
-------
204101.0         0       1       1          0       0        0      0       0
1 entry found
```

Sample Display - show fr stats signalling transmit

```
[4:1]$ show fr stats signalling transmit

                   Call                                 Release       Status
Line.LLIndex SetupProceed Connect DisconnectRelease Complete Status
Enquiry
------------ ----- ------- ------- ---------- ------- -------- ------
-------
204101.0         1   0       0          0         0       0    0       0
1 entry found
```

svcs *<options>*

Displays statistics for all SVCs or for a specified SVC.

The **show fr svc** command includes the following subcommand options:

- calls
- numbers
- priority
- shaping

The table includes the following information, depending on the subcommand option:

Line.LLIndex.DLCI	Line or instance identifier for the service record.
Call direction	States whether the call is inbound or outbound.
Circuit	Identifies the circuit.
Duration in HH:MM:SS	Duration of the call in hours, minutes, and seconds.
Number	The outbound/inbound calling number.
Subaddress	The subaddress of the calling number.
Plan	The addressing plan: X.121 or E.164.
Type	The type of number. Options are International and Unknown.
Data priority current	The current priority for this circuit.
Data priority lowest	The lowest acceptable priority for this circuit.
Gain priority current	The current gain priority for this circuit.
Gain priority lowest	The lowest acceptable gain priority for this circuit.
Keep priority current	The current keep priority for this circuit.
Keep priority lowest	The lowest acceptable keep priority for this circuit.
Inbound CIR	The CIR for inbound traffic.
Inbound Committed Burst	The committed burst value for inbound traffic.
Inbound Excess Burst	The excess burst value for inbound traffic.
Outbound CIR	The CIR for outbound traffic.
Outbound Committed Burst	The committed burst value for outbound traffic.
Outbound Excess Burst	The excess burst value for outbound traffic.

Sample Display - show svcs calls

```
[4:1]$ show fr svcs calls

                  Call                  Duration
Line.LLIndex.DLCI Dir.     Circuit      HH:MM:SS
----------------- ---- --------------- --------
204101.0.979      Out  S41             0:02:02
1 entry found
```

Sample Display - show svcs numbers

```
[4:1]$ show fr svcs numbers

                  Call
Line.LLIndex.DLCI Dir.             Number        Subaddress    Plan   Type
----------------- ----          --------------- --------------- -----
------
204101.0.979      Out  Called :          13101          12345 E.164 Unknwn
                       Calling:          13201                E.164 Unknwn
1 entry found
```

Sample Display - show svcs priority

```
[4:1]$ show fr svcs priority

                   Data Priority       Gain Priority       Keep Priority
                  ------------------- -------------------
-------------------
Line.LLIndex.DLCI  Current   Lowest    Current   Lowest    Current   Lowest
----------------- --------- --------- --------- --------- ---------
---------
204101.0.979      Unspecf'd Unspecf'd Unspecf'd Unspecf'd Unspecf'd
Unspecf'd
1 entry found
```

Sample Display - show svcs shaping

```
[4:1]$ show fr svcs shaping

                  -----------Inbound-----------
----------Outbound-----------
                          -------Burst-------          -------Burst-------
Line.LLIndex.DLCI    CIR    Committed  Excess     CIR    Committed  Excess
----------------- --------- --------- --------- --------- ---------
---------
204101.0.979             0         0 268400000         0         0 268400000
1 entry found
```

vcs [*<line>* | *<line.llindex>* | *<line.llindex.DLCI>*]

Displays information about all or selected Frame Relay virtual connections. You can use the following options with the **vcs** command:

<line>	Limits the display to the specified Frame Relay line.
<line.llindex>	Limits the display to the specified Frame Relay interface.
<line.llindex.DLCI>	Limits the display to the specified PVC. *<line.llindex>* specifies the Frame Relay interface. *<dlci>* specifies the individual PVC.

The table includes the following information:

Line.LLIndex.DLCI	Line or instance identifier for the Frame Relay interface plus the PVC identifier (DLCI).
State	State of the virtual circuit as follows: • *Invalid* - Circuit is configured but the switch has not confirmed it. • *Active* - Circuit is usable. • *Inactive* - Circuit is configured but not active.
Type	Way the virtual circuit was created: • *Static* - User manually configured the VC. • *Dynamic* - VC was created during operations. • *SVC* - A switched virtual circuit
Mode	Operational mode of the VC, as follows: • *Direct* - Upper-layer protocols view this VC as a point-to-point connection; as an individual network interface. • *Group* - Upper-layer protocols treat this VC as one of a group of destinations to the switched network. The upper-layer protocols use a single network address to send all traffic destined for the switched network to the Frame Relay network interface. • *Hybrid* - Allows protocols to view this VC as part of the group while the bridge views the VC in direct mode.
Congestion	Status of the congestion control mechanisms: Disabled, Enabled, or Inherit. Inherit indicates that the VC should use the parameters from the DLCMI record.

Serv	Circuit number of the VC, unless this is a hybrid circuit. If this is a hybrid circuit, Serv is the Circuit number of the group.
Circuit	Name of the Frame Relay circuit for the VC unless the circuit is hybrid. If this is a hybrid circuit, Circuit is the name of the hybrid circuit.

Sample Display - show fr vcs

```
$show fr pvcs
 Line.LLIndex.DLCI   State    Type    Mode   Congestion Serv    Circuit
------------------- -------- -------- -------- ---------- ----
---------------
201302.0.0         Control  Dynamic  Group    Inherit    -    S132
201302.0.100        Active   Dynamic  Group    Inherit    2    S132
201302.0.101        Active   Dynamic  Group    Inherit    2    S132
201302.0.102       Inactive Dynamic  Group    Inherit    2    S132
201302.0.103       Inactive Dynamic  Group    Inherit    2    S132
201302.0.104         Inactive Dynamic  Group    Inherit    2    S132
204101.0.0         Control  Dynamic  Group    Inherit    -    S41
204101.0.979         Active   SVC      Group    Inherit    1    S41
8 entry(s) found
```

show fwall

The **show fwall** *<option>* commands display information about the BaySecure FireWall-1 configuration.

The **show fwall** command supports the following subcommand options:

summary	interface

summary

Displays the configuration of BaySecure FireWall-1.

Sample Display – show fwall summary

```
Configured State              : enabled
Current State                 : up
Primary Management Station    : 192.32.15.76
Secondary Management Station 1: 192.32.15.75
Secondary Management Station 2: 0.0.0.0
Local Host IP                 : 172.32.1.1
Version                       : 1
```

The columns displayed have the following meanings:

Configured state	Indicates whether the firewall is enabled or disabled on the router.
Current state	Indicates whether the firewall is active or inactive.
Primary Management Station	Displays the IP address of the primary management station.
Secondary Management Station 1	Displays the IP address of the first backup management station.
Secondary Management Station 2	Displays the IP address of the seccond backup management station.
Local Host IP	Displays the IP address of the router where the firewall software is installed.
Version	Displays the version of firewall software.

interface

Displays the current state of BaySecure FireWall-1 on an interface.

Sample Display – show fwall summary

```
Slot/Port Config State   Port Type   Name
-----------------------------------------------------------
   1/1    enabled        CSMACD
   1/2    enabled        CSMACD
   1/3    enabled        SYNC
   1/4    enabled        E1
   2/1    enabled        T1
   2/4    enabled        SYNC
   6/3    enabled        TOKEN
   6/4    enabled        FDDI
  12/2    enabled        SYNC
  12/3    enabled        SYNC
  13/1    enabled        UNKNOWN
  13/2    enabled        SYNC
```

The columns displayed have the following meanings:

Slot/Port	Slot and port numbers, separated by a slash.
Config State	State of the firewall on the slot/port pair.
Port Type	Type of port
Name	Name assigned to the port.

show l2tp

The **show l2tp** *<option>* commands display information about the Layer 2 Tunneling Protocol (L2TP). For information about L2TP, refer to *Configuring L2TP Services.*

The **show l2tp** command supports the following subcommand options:

auth_info	stats
auth_statistics	tunnels
configuration	
sessions	

auth_info

Displays information about tunnel authentication for a specific L2TP interface. The display includes the following information:

Instance ID	Connector's instance identifier.
Auth Slot	Slot number used for L2TP.
Secret	Tunnel authentication password.

Sample Display - show l2tp auth_info

```
L2TP Tunnel Authentication Information
--------------------------------------

 Inst  Auth  Secret
 ID    Slot
 ----- ----- ----------
 0     0

 Total of    1 L2TP Pools.
```

auth_statistics

Displays tunnel authentication and session statistics for a specific circuit. The display includes the following information:

Slot Number	Slot number used for L2TP.
Success	Number of successful tunnel authentications attempts and sessions.
Fail	Number of failed tunnel authentication attempts.
Count	Number of active tunnels and sessions.

Sample Display - show l2tp auth_statistics

```
L2TP Tunnel Authentication Statistics Information
-------------------------------------------------

       Tunnel Authentication Session Authentication
 Slot  --------------------- ----------------------
 Num    Success  Fail  Count  Success  Fail  Count
 ----- --------  ----  ----- --------  ----  ------
 2     TUNNEL AUTH DISABLED  SESSION AUTH DISABLED

 Total of    1 L2TP Pools.
```

configuration

Displays the L2TP configuration for the router. The display includes the following information:

IP State	The LNS IP state, that is, whether or not it is active.
LNS Address	The IP address of the router serving as an LNS.
LNS Host Name	The router’s host name.
Tunnel Auth.	Indicates if tunnel authentication is enabled or disabled.

Sample Display - show l2tp configuration

```
L2TP Configuration Information
------------------------------

  IP           LNS             LNS         Tunnel
 State      Address         HostName      Auth.
 ----- --------------- --------------- ----------
 Up      192.32.16.90    BayRS           Disabled


 Total of    1 LNS instances.
```

sessions

Displays L2TP session information. The table displays the following information:

LNS Tun ID	LNS tunnel ID for the L2TP session.
LNS Call ID	LNS call ID for the L2TP session.
LAC Tun ID	LAC tunnel ID for the L2TP session.
LAC Call ID	LAC call ID for the L2TP session.
Calling Number	Phone number of the remote user.
Called Number	Phone number of the router.
Conn. Speed	Speed of the connection in b/s.
Frame Type	Framing type used in the ICCN message.
Bear Type	Bearer type used in the ICRQ message.
Chan. ID	Physical channel ID used in the ICCN message.

Sample Display - show l2tp sessions

```
L2TP Session Information
------------------------
     LNS            LAC       Calling        Called     Conn. Frame Bear
Chan.
 TunID CallID TunID CallID    Number       Number    Speed Type  Type  ID
 ----- ------ ----- ------ ------------- ------------- ----- ----- -----
-----
 16481 1      32842 49188              5084363400     64000 1     1     19

 Total of    1 L2TP sessions.
```

stats

Displays the L2TP statistics for establishing an L2TP tunnel. The display includes the following information:

Slot	Slot of the L2TP interface.
SCCRQ Valid/Invalid	Number of valid and invalid SCCRQ requests.
SCCCN Valid/Invalid	Number of valid and invalid SCCCN messages.
ICRQ Valid/Invalid	Number of valid and invalid ICRQ messages.
ICCN Valid/Invalid	Number of valid and invalid ICCN messages.

Sample Display - show l2tp stats

```
L2TP Statistics
---------------


Slot: 2

    SCCRQ            SCCCN            ICRQ             ICCN
Valid  Invalid   Valid  Invalid   Valid  Invalid   Valid  Invalid
-----  -------   -----  -------   -----  -------   -----  -------
1      0         1      0         1      0         1      0

  HELLO       StopCCN       CDN         Bad Ctrl  Bad Payload
Tx    Rx     Tx    Rx     Tx    Rx     Packets   Packets
--    --     --    --     --    --     -------   -------
0     0      0     0      0     0      0         0

Active Tunnels  =  1
Active Sessions =  1
```

tunnels

Displays the L2TP tunnel information. The display includes the following information:

Slot Num	Number of the slot for the L2TP interface.
LNS Tun. ID	Router’s tunnel ID.
LNS Address	Router’s IP address.
LAC Tun. ID	LAC’s tunnel ID.
LAC Address	LAC’s IP address.
LAC Host Name	LAC’s host name.
# of Active Sessions	Number of active L2TP sessions.

Sample Display - show l2tp tunnels

```
L2TP Tunnel Information
-----------------------

 Slot   LNS         LNS         LAC         LAC           LAC       # Active
 Num   Tun.ID     Address     Tun.ID     Address       HostName    Sessions
 ----- ------ --------------- ------ --------------- ------------
--------
 2     16481  192.32.16.90    32842  192.32.16.93    BayNetworks          1

 Total of    1 L2TP tunnel(s).
```

show lane les

The **show lane** *<options>* command displays information about ATM LAN Emulation. For a complete list of **show lane** options, see *Using Technician Interface Scripts*. For details about the Bay Networks implementation of ATM, see *Configuring ATM Services*.

The **show lane** command supports an **les [<circuit_name>]** option in the BayRS 12.10 Release.

les [*<circuit_name>*]

Displays ATM LAN Emulation Server (LES) state and address information for all circuits, or for a specific circuit.

The table displays the following information:

Cct#	Circuit number of the LEC.
Circuit Name	Circuit name of the LEC.
Inst	The instance (that is, circuit number and order of preference) for each configured LES.
State	The state of the LES (enable or disable).
LES Address	The configured ATM address of the LES that the LAN emulation client uses.

Sample Display - show lane les

```
ATM LAN Emulation LEC-LES Table
-------------------------------

 LEC: Cct#3     LAN Name lan1
-------------------------------------------
 Inst  State   LES Address
 ----  -----   -----------
 3.1   Enable  39.30.00.00.00.00.00.00.00.00.00.40.0B.01.BC.80.00.01
 3.2   Enable  39.20.00.00.00.00.00.00.00.00.00.40.0B.01.01.80.1E.01
 3.3   Enable  39.50.00.00.00.00.00.00.00.00.00.45.0B.AF.83.80.00.01

 LEC: Cct#4     LAN Name lan2
-------------------------------------------
 Inst  State   LES Address
 ----  -----   -----------
 4.1   Enable  39.30.00.00.00.00.00.00.00.00.00.40.0B.01.BC.80.01.01
 4.2   Enable  39.20.00.00.00.00.00.00.00.00.00.40.0B.01.01.80.1B.01
 4.3   Enable  39.50.00.00.00.00.00.00.00.00.00.45.0B.AF.83.80.01.01
```

show mospf

The **show mospf** *<option>* command displays information about OSPF multicast extensions (MOSPF). For detailed information about the Bay Networks implementation of MOSPF, refer to *Configuring IP Multicasting and Multimedia Services.*

The **show mospf** command supports group address arguments for the **fwd** command option in BayRS 12.10.

fwd

Displays the following information from the MOSPF forwarding database:

Group	Multicasting group
Source	The multicasting source
Upstream Interface	The IP address of the upstream interface
Downstream Interface	The IP address of the downstream interface

In addition, you can add a group address argument to the **fwd** subcommand. This limits table entries to those matching the argument. The argument can contain the wildcard character, "*****", for example:

show mospf fwd	Shows forwarding entries for all group addresses
show mospf fwd 224.2.*	Shows forwarding entries for all group addresses starting with 224.2
show mospf fwd 225.3.12.1	Shows the forwarding entry for the group address 225.3.12.1

Sample Display - show mospf fwd 224.128.128.*

```
MOSPF Forwarding Database
-------------------------
                                    Upstream
     Group           Source         Interface
---------------  ---------------  ---------------
224.128.128.10   201.1.1.0        201.1.1.1
  downstream:  201.0.2.1 (3)
224.128.128.10   201.2.1.0        201.0.2.1
  downstream:  201.1.1.1 (1)
224.128.128.11   201.1.1.0        201.1.1.1
  downstream:  201.0.2.1 (3)
224.128.128.11   201.2.1.0        201.0.2.1
  downstream:  201.1.1.1 (1)
      .                .                .
      .                .                .
      .                .                .
```

show ospf

The **show ospf** *<option>* commands display state, configuration, and statistical information about the Open Shortest Path First (OSPF) protocol. For details on the Bay Networks implementation of OSPF, refer to *Configuring IP Services*.

The **show ospf base** command displays a new ASE Metric Support column, and the **show ospf interfaces** command indicates a new interface type, "passive."

base

Displays global information for the OSPF router. The base record controls OSPF for the entire system. The table includes the following information:

Router Id	Router identifier, which is unique among all OSPF routers.
State	State of the protocol: Disabled, Down, Init (initializing), Not Pres (enabled but not yet started), or Up.
Area Border Router	Whether or not the router is an area border router: Yes or No.
AS Boundary Router	Whether or not the router is an Autonomous System boundary router: Yes or No.
Slot Running Primary	The slot on which the OSPF soloist is running, and where the Link State Database exists. (If the Primary soloist goes down, the router attempts to use the Backup soloist.)
Slot Running Backup	The slot on which the backup OSPF soloist is running.
ASE Metric Support	Whether or not ASE metric support is enabled or disabled. (This metric is not compatible with OSPF ASE metrics used prior to Version 8.0 of the router software.)
ASE Default Tags	How tags are generated for ASEs unaltered by an export route filter or an announce route policy: • *Default (1)* - Use a value of zero. • *Automatic (2)* - Generate an automatic tag, per RFC1403. • *Proprietary (3)* - Use the next hop for IGP routes and the neighbor AS for EGP routes (Wellfleet proprietary scheme).

Hold Down Time	Hold-down timer for calculating the Shortest Path First (SPF, Dijkstra) algorithm. Determines how often the algorithm runs. A value of zero means no hold down.
Slot Mask	Identifies slots on which OSPF can run. The MSB represents slot 1; the next significant bit represents slot 2; and so on.

Sample Display - show ospf base

```
OSPF Base Information
---------------------

                              Area    AS        Slot     Slot     ASE
                              Border  Boundary  Running  Running  Metric
Router ID        State        Router  Router    Primary  Backup   Support
---------------  -----------  ------  --------  -------  -------  -------
1.1.1.1          Up           No      No        3        None     Disable

ASE Default Tags:       Zero
Hold Down time[sec]:    1
Slot Mask:              0xFFFC0000
```

interface

Displays a table of OSPF interfaces. The table includes the following information:

IP Address	Internet address of the OSPF interface.
Area Id	Identifier of the area where the interface belongs.
Type	Type of interface link, as follows: • *PtoP* - Point-to-Point interface. • *BCAST* - Broadcast network. • *NBMA* - Non-Broadcast Multi-Access network. • *PASS* - Passive interface (accepts no hello packets; issues no advertisements or hello packets; forms no neighbor relationships). • *DFLT* - Not configured appropriately. Point-to-multipoint is needed.

State	State of the interface, as follows: • *Down* - Interface is not operational. • *Waiting* - Interface is waiting. • *P to P* - Interface is in Point-to-Point state; occurs when the type is Point to Point. • *DR* - Router is the Designated Router on this network. • *BackupDR* - Router is the Backup Designated Router on this network. • *DR Other* - Router is neither the DR nor the BDR on this network.
Metric	Cost of using this interface.
Priority	Router's priority on this interface, used in multiaccess networks (Broadcast or NBMA) for electing the designated router. If the value is 0, this router is not eligible to become the designated router on this network.
Designated DR/Backup DR	Two IP addresses for each interface. The first address is the IP address of the Designated Router on the network. The second address is the IP address of the Backup Designated Router on this network. Point-to-Point links do not contain a Designated Router or Backup Designated Router.

Sample Display - show ospf interface

```
OSPF Interfaces
---------------

                                                                  Designated DR/
 IP Address      Area Id    Type  State    Metric Priority      Backup DR
 ----------      -------    ----  -----    ------ -------  ---------------
 192.32.174.65   0.0.0.0    PtoP  P to P       10       1   0.0.0.0
                                                            0.0.0.0

 192.32.174.97   0.0.0.0    BCAST BackupDR      1       1   192.32.174.98
                                                            192.32.174.97

 1.1.1.1         0.0.0.0    PASS  Waiting       1       1   0.0.0.0
                                                            0.0.0.0
```

show ppp

The **show ppp** command supports a **ccp** option in the BayRS 12.10 release.

ccp {**configured** | **negotiated**}

The **show ppp ccp** command shows the compression algorithm that is configured on the local router and the algorithm that is actually negotiated with the peer router. The display for both **ccp configured** and **ccp negotiated** includes the following information:

Circuit	The name of the active circuit.
State	Indicates whether the Compression Control Protocol (CCP) is initialized.
Type	The CCP type: CCP (listed as Normal in the display) or ILCCP.
Option	The compression protocol: Any, WCP, or Stac LZS.

configured Displays the compression algorithm configured for the router.

Sample Display - show ppp ccp configured

```
PPP: Compression NCP Configured Information
-------------------------------------------

 Circuit   State    Type             Option
 -------- -------- ---------------- --------
 S41      Initial  Normal           Any

 1 Entry found.


1 Total Entries found.
```

negotiated Displays the compression algorithm actually negotiated with the peer router.

Sample Display - show ppp ccp negotiated

```
PPP: Compression NCP Negotiated Information
-------------------------------------------

 Circuit  State    Type             Option
 -------- -------- ---------------- --------
 S41      Opened   Normal           OUI (WCP)

 1 Entry found.


1 Total Entries found.
```

show sr

The **show sr** commands display information about source routing interfaces. For detailed information on source routing, refer to *Configuring Bridging Services.*

The **show sr** command supports the following new subcommand option:

traffic filters

traffic filters

Displays any traffic filters on a source routing interface. The table indicates whether or not traffic filters are operating and includes the following information:

Circuit	The name you assign to the circuit.
Mode	The mode of the SR traffic filter: Enabled or Disabled.
Status	The state of the SR traffic filter: Active or Inactive.
Rule Number	The order in which the router applies the rules.
Fragment Number	The number assigned to each rule by the router.
Filter Name	A character string that describes the rule.

show stac

The **show stac** *<option>* commands display information about the Stac LZS data compression service. For information about Stac LZS, refer to *Configuring Data Compression Services*.

The **show stac** command supports the following subcommand options:

circuits [circuit <circuit name>]
stats [errors] [<circuit number>]

circuits [circuit <*circuit name*>]

Displays the state of all circuits and the type of compression for each circuit. The display includes the following information:

Circuit Name	Name of the circuit.
Circuit Number	Connector's instance identifier.
Enable	State of the circuit, either enabled or disabled.
Compression Mode	Compression mode that is negotiated. These modes are defined by 1974. For Stac, this will always be mode 3.
Cfg Engine Type	Engine type configured. The engine type can be software or hardware compression.

Sample Display - show stac circuits

```
STAC Circuit Entries
--------------------
                                        Cfg
 Circuit Circuit          Compression  Engine
  Name    Number  Enable      Mode      Type
-------- ------- -------- ----------- -------
S22            2 Disabled    Mode 3     Sw

1 STAC circuit(s) configured.
```

stats [errors] [<*circuit number*>]

Displays Stac LZS statistical information for a specified circuit. The display includes the following information:

Circuit	Name of the circuit.
Compression Ratio	Compression ratio, which is the size of uncompressed data compared with the size of the same data after it is compressed.
Decompression Ratio	Decompression ratio, which is the size of decompressed data compared with the size of the same data before it is decompressed.
Compressor In	Number of bytes input to the software compression library.
Compressor Out	Number of bytes output by the software compression library.
Decompressor In	Number of bytes input to the decompression software library.
Decompressor Out	Number of bytes output to the decompression software library.
CPC Packets Transmitted	Number of continuous-packet compression packets transmitted by Stac LZS.
CPC Packets Received	Number of continuous-packet compression packets received by Stac LZS.

Note that if you take the Compressor In number and divide it by the CPC Packets Transmitted number, you get an estimate of the compression packet size.

Sample Display - show stac stats

```
STAC Performance And Data Statistics
------------------------------------

         Compression Decompression
Circuit     Ratio        Ratio
-------- ----------- -------------
S22           3.5:1        3.5:1

   Compressor   Compressor  Decompressor Decompressor
       In           Out          In           Out
  ------------ ------------ ------------ ------------
        137356        38892        38957       137356

   CPC Packets  CPC Packets
   Transmitted   Received
  ------------ ------------
          2986         2986

1 Entry.
```

show sync

The **show sync** *<option>* commands display configuration, status, and statistical information about synchronous (SYNC) lines. For a complete list of **show sync** options, see *Using Technician Interface Scripts*. For detailed information about configuring synchronous lines, refer to *Configuring WAN Line Services*.

The **show sync** command supports new **ft1_config** and **ft1_state** options in the BayRS 12.10 Release.

ft1_config

Displays configuration details of the FT1/T1 DSU/CSU adapter module. Use this command to verify the information that has been set for FT1 operations. The table includes the following information:

Line Type	Frame format used on the T1 line, as follows: • *SF* - Superframe. • *ESF* - Extended Superframe.
Line Coding	Line coding configured for the FT1/T1 DSU/CSU adapter module, as follows: • AMI - Alternative Mark Inversion transmits a binary 0 as 0 volts and a binary 1 as either a positive or negative pulse with the opposite polarity of the previous pulse. With AMI coding, the adapter module remains in frame synchronization for 45 consecutive zeros. • *B8ZS* - Bipolar 8 Zero Substitution replaces a block of eight consecutive binary zeros with an 8-bit B8ZS code containing bipolar violations in the fourth and seventh bit positions of the substituted code in a transmitted message. When a message is received, this action is reversed: the B8ZS code is replaced with eight consecutive binary zeros.
Loop Config	Indicates the loopback setting as follows: • *Line Loopback* - Loops received data back onto the T1 transmission path at the point where the T1 interface enters the FT1/T1 DSU/CSU adapter module. • *Payload Loopback* - Detects and encodes an ANSI Bit-Oriented Payload Loopback message or an AT&T Payload Loopback message across the T1 Facility Data Link (FDL). Upon detection of a Payload Loopback message, the FT1/T1 DSU/CSU adapter module transmits the received information in the outgoing direction. • *No Loop* - No loopback is configured on the FT1/T1 DSU/CSU adapter module.
FDL Configuration	Defines the type of Facility Data Link (FDL) configured, as follows: • *ANSI403* - ANSI Publication T1.403 • *ATT54016* - AT&T Publication 54016
Primary Tx Clock	Defines the type of primary T1 transmit timing source used, as follows: • *Loop* - Timing from the T1 port. • *Local* - Internal timing from the FT1 adapter module.

Secondary Tx Clock	Defines the type of secondary T1 transmit timing source to be used when a T1 primary transmit clock fails: • *Loop* - Timing from the T1 port. • *Local* - Internal timing from the FT1 adapter module.
Current Tx Clock	Defines the T1 transmit timing source currently configured: • *Loop* - Timing from the T1 port. • *Local* - Internal timing from the FT1 adapter module.
Rate	Number of bits per second at which voice, data, and video signals are transmitted over the T1 line.
DS0 Map	DS0 channels configured for the DS1 frame; ranges from 1 to 24.

Sample Display - show sync ft1_config

```
Configuration of FT1 card in Slot 1 Connector 1:
------------------------------------------------
Line Type: ESF
Line Coding: B8ZS
Loop Config: No Loop
FDL Configuration: ANSI403
Primary Tx Clock: Loop
Secondary Tx Clock: Local
Current Tx Clock: Loop
Rate: 1536000
DS0 Map: 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24

    1 entry(s) found
```

ft1_state

Displays information about the operational state of the FT1/T1 DSU/CSU adapter module. The table includes the following information:

Slot	Slot identifier; always 1 for the ARN.
Conn	Connector identifier; ranges from 1 to 2.
Port State	State of the port associated with the FT1/T1 line, as follows: • *Red Alarm* - A red alarm signal, indicating the loss of T1 framing. • *Yellow Alarm* - A yellow alarm signal from the T1 network indicating that the remote T1 interface is out-of-frame. • *Loopback* - Port is in loopback mode. • *Up* - Port is synchronized with the T1 network. • *AIS* - A blue alarm signal from the T1 network indicating a total loss of signal from the remote T1 device.
Loopback State	Defines the loopback state of the port, as follows: • *Line Loopback* - Loops received data back onto the T1 transmission path at the point where the T1 interface enters the FT1/T1 DSU/CSU adapter module. • *Payload Loopback* - Detects and encodes an ANSI Bit-Oriented Payload Loopback message or an AT&T Payload Loopback message across the T1 Facility Data Link (FDL). Upon detection of a Payload Loopback message, the FT1/T1 DSU/CSU adapter module transmits the received information in the outgoing direction. • *No Loop* - No loopback is configured on the FT1/T1 DSU/CSU adapter module.

Sample Display - show sync ft1_state

```
Slot  Conn  Port State    Loopback State
----  ----  ----------    ---------------
 1      1   Yellow Alarm  No Loop

1 entry(s) found
```

stac enable/disable

Use the Stac enable command to enable Stac LZS for a specific interface. Use the Stac disable command to disable Stac LZS.

enable

Indicates if Stac LZS is enabled for a specific interface.

Sample Display - stac enable circuit 2

```
STAC circuit 2 enabled.
```

disable

Indicates if Stac LZS is disabled for a specific interface.

Sample Display - stac disable circuit 2

```
STAC circuit 2 disabled.
```

Using Technician Interface Software

The following section is an amendment to *Using Technician Interface Software.*

Output Change to ping -p

The **ping** command sends an Internet Control Message Protocol (ICMP) echo request to the remote address you specify. The remote device responds if it can be reached, and the console displays the response or the result of the request. By adding **-p** to this command, the ping program generates a path trace report that displays the intervening hop addresses to the destination and the time it takes to reach them.

The output of the **ping -p** command has changed. The new output is as follows:

```
[1:1]$ ping -p 192.32.13.200

traceroute to 192.32.13.200: 1-30 hops, 16 byte packets

 1 193.32.44.57  11 ms  7 ms  7 ms

 2 193.32.44.12  9 ms  8 ms  15 ms

 3 193.32.60.41  10 ms  10 ms  10 ms

 4 192.32.13.200  11 ms  11 ms  11 ms
```